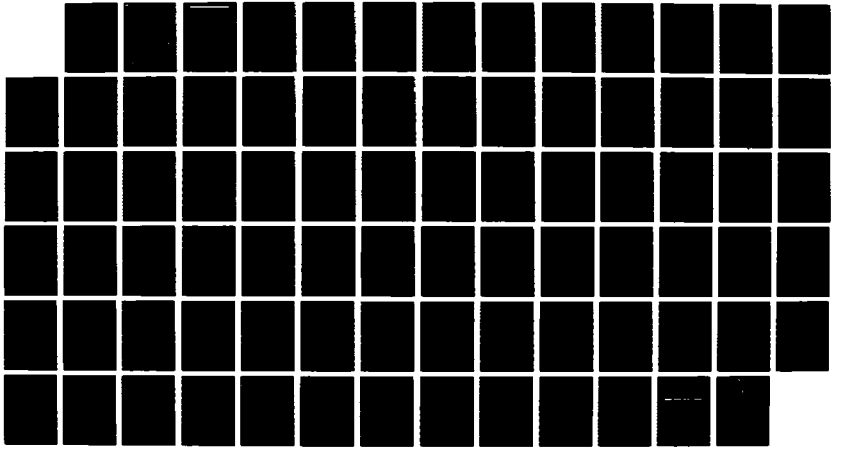
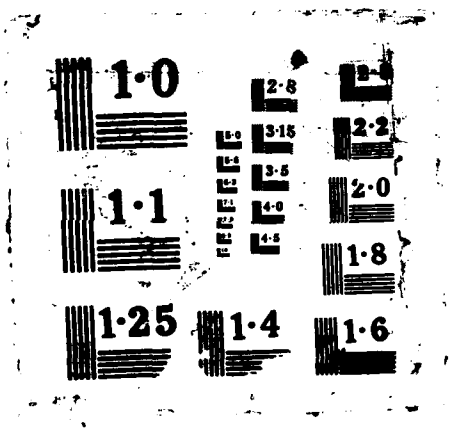
AD-A185 235 MICROCOMPUTER SECURITY ISSUES IN AN OFFICE ENVIRONMENT 1/1
(U) DAVID W TAYLOR NAVAL SHIP RESEARCH AND DEVELOPMENT
CENTER BET.. I S ZARITSKY NOV 86 DTNSRDC/CMLD-86/43

UNCLASSIFIED F/G 12/8 NL




1·0
1·1
1·25
1·4
1·6
1·8
2·0
2·2
2·8
3·15
3·5
4·0
4·5

(12)

**David W. Taylor Naval Ship Research and Development Center**

Bethesda, MD 20084-5000



DTNSRDC/CMLD-86/43 November 1986

Computation, Mathematics, and Logistics Department

Departmental Report

# MICROCOMPUTER SECURITY ISSUES IN AN OFFICE ENVIRONMENT

by

Irving S. Zaritsky

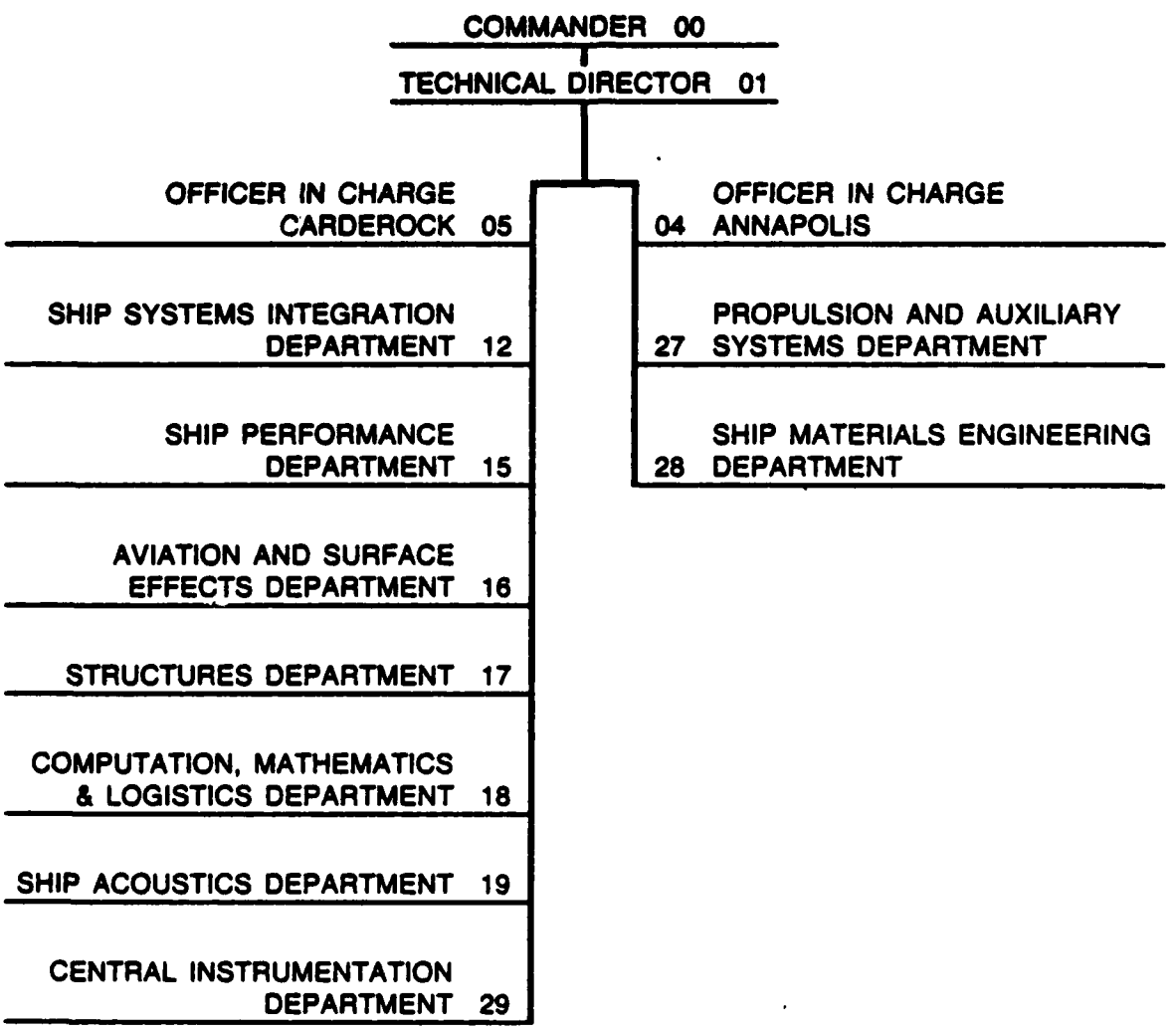


Approved for Public Release: Distribution unlimited.

MICROCOMPUTER SECURITY ISSUES IN AN OFFICE ENVIRONMENT

DTNSRDC/CMLD-86/43

# MAJOR DTNSRDC TECHNICAL COMPONENTS




**DESTRUCTION NOTICE** — For **classified** documents, follow the procedures in DOD 5220.22M, Industrial Security Manual, Section II-9, or DOD 5200.1-R, Information Security Program Regulation, Chapter IX. For **unclassified**, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

AD-A185 235

# REPORT DOCUMENTATION PAGE

| | |
|---|---|
| 1a. REPORT SECURITY CLASSIFICATION<br>UNCLASSIFIED | 1b. RESTRICTIVE MARKINGS |
| 2a. SECURITY CLASSIFICATION AUTHORITY | 3. DISTRIBUTION/AVAILABILITY OF REPORT<br>APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED |
| 2b. DECLASSIFICATION/DOWNGRADING SCHEDULE | |
| 4. PERFORMING ORGANIZATION REPORT NUMBER(S)<br>DTNSRDC/CMLD-86/43 | 5. MONITORING ORGANIZATION REPORT NUMBER(S) |
| 6a. NAME OF PERFORMING ORGANIZATION<br>David Taylor Naval Ship R&D Center<br>6b. OFFICE SYMBOL (If applicable)<br>Code 1824 | 7a. NAME OF MONITORING ORGANIZATION<br>Naval Supply Systems Command Code PML 5505 |
| 6c. ADDRESS (City, State, and ZIP Code)<br>Bethesda, MD 20084-5000 | 7b. ADDRESS (City, State, and ZIP Code) |
| 8a. NAME OF FUNDING/SPONSORING ORGANIZATION<br>8b. OFFICE SYMBOL (If applicable) | 9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER |
| 8c. ADDRESS (City, State, and ZIP Code) | 10. SOURCE OF FUNDING NUMBERS<br>PROGRAM ELEMENT NO. / PROJECT NO / TASK NO. / WORK UNIT ACCESSION NO. |

11. TITLE (Include Security Classification)
MICROCOMPUTER SECURITY ISSUES IN AN OFFICE ENVIRONMENT

12. PERSONAL AUTHOR(S)
Irving S. Zaritsky

| 13a. TYPE OF REPORT | 13b. TIME COVERED | 14. DATE OF REPORT (Year, Month, Day) | 15. PAGE COUNT |
|---|---|---|---|
| Final | FROM 86 Jan TO 86 Sep | | 74 |

16. SUPPLEMENTARY NOTATION

| 17. COSATI CODES | | | 18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | |
| | | | |
| | | | |

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The purpose of this report is to aid management in establishing policy and procedures which provide security for microcomputers and unclassified but sensitive information used by these machines in an office environment.

| | |
|---|---|
| 20. DISTRIBUTION/AVAILABILITY OF ABSTRACT<br>☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS | 21. ABSTRACT SECURITY CLASSIFICATION<br>UNCLASSIFIED |
| 22a. NAME OF RESPONSIBLE INDIVIDUAL<br>Irving S. Zaritsky | 22b. TELEPHONE (Include Area Code)<br>(202) 227-1889<br>22c. OFFICE SYMBOL<br>Code 1824 |

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted
All other editions are obsolete

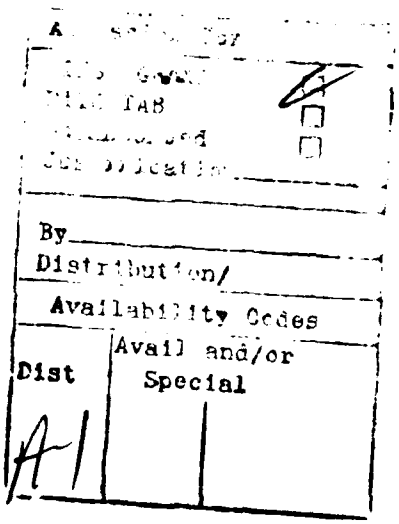
SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

CONTENTS

## APPENDICES





## ABSTRACT

This report presents the issues which management must address in establishing policy and procedures to provide physical security for microcomputers and protection for unclassified but sensitive information used by these machines in an office environment. Although recommendations are also provided, this report is not intended to be a handbook on formal risk analysis.


## ADMINISTRATIVE INFORMATION


The Computer Science and Information Systems Division of the Computation, Mathematics, and Logistics Department prepared this report for the David Taylor Naval Ship Research and Development Center. This report was sponsored by the Naval Supply Systems Command, Code PML 5505 under work unit 1870-702.


## SCOPE

The scope of this report is limited to the following areas:

- Protection of sensitive but unclassified data in an office environment.
- Protection of hardware from theft and electrical power line anomalies.

This report does not cover the following topics:

- Physical hazards such as fire or water damage.
- Environmental issues such as pollution, temperature or humidity.
- TEMPEST issues such as electromagnetic emanation control.
- Mainframe issues are briefly addressed.

Note also that the product survey implies no endorsements and that the product survey is not a comprehensive listing but instead attempts to display a range of products in order to match the desired level of security with the available resources.

# INTRODUCTION

This report presents the issues which management must address in establishing policy and procedures to provide physical security for microcomputers and protection for unclassified but sensitive information used by these machines in an office environment. Although recommendations are also provided, this report is not intended to be a handbook on formal risk analysis.

PCs are appearing in offices everywhere. They are excellent productivity tools. With a PC, information can be easily accessed, modified, or destroyed. Unfortunately, this means that sensitive data is potentially at risk. When PCs are shared, the risk is higher, and when the PCs are in an open, accessible office environment, the risk to the equipment itself may be significant.

Management can best deal with this situation by appointing an Office Information System Security Officer (OISSO) as a driving force (an individual or group depending on the size of the organization) to be permanently responsible and accountable for the security of PCs and sensitive data. The OISSO must be given the authority and the resources to set and carry out clearly defined policy and procedures. The OISSO must determine what degree of security is adequate.

Although PC security requires the use of technology, it is largely a human issue as it requires end user awareness, common sense, and extra effort of the kind which does not produce "products" or "results". The notion of security on a PC runs counter to most end users' view of the PC as an easy to use productivity tool. However, employees will usually go along with reasonable measures when management invokes "enlightened self-interest".

According to Zimmerman[1] threats to information security can be viewed as either actions of malicious intent or human error and natural accident. Furthermore, 95% of the PC security problem falls into one of three categories:

1. Data loss due to lack of proper backups
2. Data disclosure because they are being left exposed and unprotected from theft.
3. Information which is invalid and unreliable due to the lack of installation of quality-control mechanisms.

To the degree that technology will provide security, management should be aware that a range of protections is necessary. This should include hardware and software (for encryption and logical access control), configuration control, physical access control and if needed, electromagnetic emanation control.

## NATIONAL COMPUTER SECURITY CENTER (NCSC) CLASSIFICATIONS

### EVALUATION CRITERIA

The National Computer Security Center (NCSC), which is part of the National Security Agency (NSA) has been tasked to establish computer security standards and study and implement secure computer technology. To that end, NCSC has issued a DoD standard, nicknamed the "Orange Book", called the DoD Trusted Computer System Evaluation Criteria.[2] Five other manuals by NCSC, listed in the bibliography in Appendix A, supplement the Orange Book, and address PC security considerations, password management, and the use of magnetic media. These manuals are alternately referred to as the "Rainbow" or "Jello Series".

Computer security, as described in the Orange Book, is rated by levels of trust. There are four levels or divisions: A, B, C, and D where hardware and software with an A rating represents the most comprehensive security and a D rating represents systems with minimal or no security. Within each division, there are numeric subdivisions resulting (currently) in eight classes. Ranging in descending order of security confidence, they are "Beyond A1", A1, B3, B2, B1, C2, C1, and D.

Within each class, there are four major sets of criteria. The following is excerpted from the Orange Book:

1. POLICY

a. SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system. Given identified subjects [such as an individual or an information seeking device or process] and objects [such as data] there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object.

b. MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity, and/or the modes of access accorded those subjects who may potentially access the object.

2. ACCOUNTABILITY

a. IDENTIFICATION [and AUTHENTICATION] - Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer system and be associated with every active element that performs some security relevant action in the system.

b. ACCOUNTABILITY - Audit information must be selectively kept and protected so that the actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations.

3. ASSURANCE

a. ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements [1.a through 2.b] above. In order to assure that the four requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer system, there must be some identified and unified collection of hardware and software controls that perform those functions.

b. CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer system can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion.

4. DOCUMENTATION

This requirement describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class.

The NCSC security classifications which pertain to PCs now and in the near future are D, C1, C2, and B1. The following are excerpts from the Orange Book:

Division D: Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Division C: Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection and accountability of subjects and the actions they initiate, through inclusion of audit capabilities.

Class C1: Discretionary Security Protection. The TCB [trusted computing base] of class C1 systems nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class C1 environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class C2: Controlled Access Protection. Systems in this class enforce a more finely grained discretionary access control than class C1 systems, making users individually accountable for their actions through logic procedures, auditing of security-relevant events, and resources encapsulation.

Division B: Mandatory Protection. The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Class B1: Labeled Security Protection. Class B1 systems require all the features required for class C2. In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

As part of the classification effort, NCSC has created the Information Security Products and Services Catalogue[3]. This catalogue includes the following:

a. The Endorsed Cryptographic Product List (classified or sensitive unclassified data security)

b. The NSA Endorsed Data Encryption Standard (DES) Products List (sensitive, but unclassified data security).

c. The Protected Services List (Protected Telecommunications Services via Commercial Common Carriers).

d. The Evaluated Product List for COMPUSEC (computer security) devices.

e. The U.S. Government Preferred Products List for TEMPEST (electromagnetic emanation security) devices.

This catalogue is available directly from NCSC. Contacts are listed in Appendix B, "Key Organizations and Security Cosultants."

## NCSC PC SECURITY PERSPECTIVE

Not surprisingly, NCSC's main thrust, historically, has been the protection of DoD information on mainframe computers. However, they are also actively addressing PC security issues. They have issued a manual, nicknamed the "Powder Blue Book", called Personal Computer Security Considerations.[4] In summary, the manual is not presented as a formal policy document "but to raise the computer security awareness of the reader." Also, PCs have generally been designed and developed without much consideration for security issues. With respect to security, the DOS operating system, for example, is weak since any file on the system can be accessed by anyone with physical access to the PC. [This is discussed in some detail in the section on Using DOS.] Furthermore, most PCs lack built-in hardware mechanisms needed to isolate PC users from sensitive, security related system functions. As stated in the manual:

> "The typical personal computer is a single-state machine and therefore does not support the following security mechanisms common to larger systems:
>
> - Multiple processor states - enabling separate "domains" for users and system processes;
>
> - Privileged instructions - limiting access to certain functions (e.g., reading and writing to disk) to trusted system processes; and
>
> - Memory protection features - preventing unauthorized access to sensitive parts of the system."

The Intel 8086 and 8088 processors fall into this category. One must conclude, therefore, that NCSC would give IBM PCs, PC/XTs, and clones using DOS 2.x or 3.x a D security classification. It should be further noted that no products for the PC have received a C2 or greater classification at this time, although several products include C1 and C2 rated features. Also, although no products for the PC have been accepted on the "Evaluated Products List", some have been evaluated and reports ("features lists") are available directly from NCSC. Due to the already described lack of security features in the PC architecture, it is likely that these products will not be given classifications such as C2 or C1 but instead presented in the context that they provide additional barriers to access to the PC.

Although not mentioned in the manual, the Intel 80286/80386 processors essentially provide these features. As a result, it is possible that a PC with either of these processors and a more secure operating system than DOS 3.x may be capable of a security classification as high as B1 or B2. The successor to DOS, OS/2 will be a protected mode operating system, and will not run on 8086/8088 processors. This would probably provide sufficient justification for procurement of a PC/AT class computer instead of a PC/XT or clone.

## MANAGEMENT POLICY AND PROCEDURES

Management policy and procedures are the most important aspects of PC security. The reason is twofold. Employees may not be aware of the scope of the problem and/or may see PC related security measures as anti-productive.

Management should consider the following steps:

a. Policy and procedures must be formalized, written down and well advertised. As an example, DTNSRDC's policy and procedures for PCs are listed in Appendicies F, G, and H. This policy was derived from OPNAVINST 5239.1A by John Hays, DTNSRDC ADPSO (Code 004). Appendix F lists operating procedures. Appendix G is an ADP security survey and accreditation support data form and is an example of a risk analysis for PCs. Appendix H lists DTNSRDC's request to PC users for their contingency plan.

b. An Office Information System Security Officer (OISSO) must be appointed to be the driving force to set standards and guidelines, plan, implement, and carry out security measures. The OISSO must be given the authority, the resources, and management backing to do the job.

c. Coordinate the efforts of the OISSO with the ADP Policy Office, the physical plant security officer (PSO), the data base administrator (DBA), and the personnel department in order to define a corporate policy. This policy should include, but not be limited to the following:

(1) Accountability. Employee accountability for information loss or compromise should be well defined. PCs, security hardware and software, sensitive programs, and data should be assigned to individual owners who would be responsible for their protection. Also, accountability should focus on malicious conduct since even the best of employees are capable of error.

(2) Configuration Control. A "PC compatibility baseline" should be established. As discussed previously, PCs based on the Intel 8088 or 8086 processors (such as the IBM PC and PC/XT) are not considered secure by the NCSC. PCs based on the Intel 80286 or 80386 processors (such as the IBM PC/AT or Compaq Deskpro 386), however, are potentially more secure. Do not allow the purchase of any PC hardware or software which falls outside of this guideline. Obviously, exceptions must be allowed for special purpose situations. Also, where feasible, sensitive functions and data should be migrated to compatible micros. This is not easily accomplished but is necessary so that security oriented hardware and software are consistent agency-wide. Furthermore, this facilitates backup, recovery, maintenance, and training. [The IBM PC/XT/AT family of microcomputers have become a de facto industry standard and the issue has become the degree of compatibility of other vendors' microcomputers.]

(3) Backup. Do not allow the purchase of any hard disk based PC without adequate backup either built in (in the form of a removable cartridge unit or a streaming tape device) or added on (in the form of backup software). This is discussed in further detail in the section on Disaster Recovery.

(4) Focus. Policy should be clear as to what types of information are considered sensitive and therefore to be protected. An approximate dollar value should be assigned to all hardware, software, and data since protection schemes should not cost more than the value of the items being protected. This is discussed further in the section on Risk Analysis.

(5) Authorization. PCs located in accessible areas should have an authorized user list posted on the PC.

(6) Attidude. To set the proper tone, each user (or each PC) should have a separate, legal copy of the software he or she uses as determined by the copyright for that software. This should be coupled with an enforceable software piracy policy. Also, users should be allowed to sign out for hardware and software for use at home. One way to solve this problem is to make it easy and quick to obtain the software. This can be done by allowing the organization's "Information Center" or "User Services" group to buy a site license or network copy or simply stock several copies of endorsed software.

(7) Data Integrity. As data integrity may be considered a side issue of security, management must ensure that any decision-making done on the basis of PC generated results use programs and data which have been independently verified for accuracy.

## OFFICE INFORMATION SYSTEM SECURITY OFFICER (OISSO)

The key to an effective security program is the designation of the Office Information System Security Officer (OISSO). This may be an individual who has other tasks within the organization or an entire group as determined by the size of the organization and perceived problem. The OISSO's main responsibility should be to promote security awareness. As part of his job, he should:

a. Work with management and at least some active users to establish clear security policy and procedures.

b. Perform an informal risk analysis in order to:
- Identify potential threats
- Determine how to deal with these threats in a cost-effective & effort-effective manner.

This is discussed further in the section on risk analysis.

c. Establish a disaster recovery program. This is discussed further in the section on disaster recovery.

d. Work with management, the ADP Policy Office (ADPPO), the physical plant security officer (PSO), and the data base administrator (DBA) to create a subject-object (access rights) control matrix in order to determine physical area, hardware, data, program, and port access levels for all employees.

f. Ensure that locked areas and/or cabinets are available for all media containing sensitive information. Specially colored labels and jackets should be used to identify those media.

g. Work with management, the ADPPO, the PSO, and the DBA to determine:
- -Methods for control of physical access to computers and the areas where the are located.
- -Consistent agency-wide methods for control of program, data, and port access.
- -Which programs and data are considered sensitive. A specific custodian should then be assigned responsibility for each program and data set.
- -Policy on selection and standardization of micro hardware and software. Admittedly, this is hard to implement but it is even less desirable to buy and support different security hardware and software systems. At least some end users should be included in this process.

h. Set up a security information clearinghouse or library which might include information from:
- -Government, DoD, and agency-wide instructions
- -NBS, NCSC guidelines, publications, and films
- -Other security related publications and trade journals
- -Current vendor products
- -Schedules of courses, seminars & conferences

i. Establish a security incident reporting system.

j. Work with the Industrial Facilities department to resolve environmental issues such as electrical power line protection. For example, they must determine whether solutions should be plant-wide, building-wide, or machine-specific.

k. Work with the personnel department and the DBA to establish check-out procedures when an employee quits to ensure:
- -Timely changes are made in passwords, keys, combinations, and phone numbers listed in directories of call-back modems
- -Return and integrity of documents, hardware, software, and data

l. Consult with users frequently. This is to ensure that the measures and products are effective and not being degraded by the addition of new technology.

m. Conduct periodic audits and inspections. An occasional random site visit may discourage carelessness among end users. Also, if a logical access control device is used, and it has an internal audit (audit trail of login attempts, program and data file requests), it should be checked periodically for denied accesses.

n. Establish a training program on security awareness and data backup methods.

o. Establish specific policy with respect to:
- -Location of stored sensitive data
- -Encryption use and type
- -User IDs and passwords on PCs
- -Auditing of computer usage on PCs
- -Port access methods and choice of data line phone numbers
- -Data integrity

As an aid to the OISSO, a short bibliography of NCSC and NBS guidelines are listed in Appendix A. A brief list of knowledgeable individuals at NCSC and NBS along with some security consultants is given in Appendix B. Appendix C includes a list of institutions which offer security related training and Appendix D lists some conferences on computer security which are coming up in the near future.

As a further aid to the OISSO, NBS-ICST runs a security special interest group on their MEIE electronic bulletin board. The phone numbers are:

data: (301) 948-5718 [8-1-N]
sys-op: (301) 975-3359

Another security interest electronic bulletin board is sponsored by the Communications Security Association. The phone numbers are:

data: (301) 843-9266 [7-1-N]
sys-op (703) 528-4229 [Paul Bowling]

## RISK ANALYSIS

### Overview

Risk analysis is the process of evaluating the existing controls on existing ADP resources along with the threats and vulnerabilities of existing and future (ADP) resources in terms of replacement cost and cost (both tangible and intangible) to an organization as a result of disclosure or modification of data. Risk assessment is essentially a risk analysis performed only on existing resources. If the information were classified, the result of such an analysis would be an NCSC computer security classification such as B1 or C2. Otherwise, a risk analysis would result in a series of responses such as "improve physical access control using smartcards or biometrics". The OISSO would then take those measures deemed most cost-effective. The cost to protect the resources should not exceed the value of those objects.

There are several, very expensive, risk analysis software packages available. Most of these run on an IBM PC. Listings of these products can be found in an article by Hoffman[5] and the Datapro Reports on Information Security[6]. Although it was rejected by NAVDAC, NCSC has a free software program called LAVA (Los Alamos Vulnerability Assessment) which may be helpful. An approach to determining computer security requirements for Navy systems is described by Landwehr and Lubbes[7].

It is the opinion of this author that while these formal, rigorous methodologies are appropriate for larger systems, they would not be cost-effective for evaluating a PC-based environment. According to Adolph Cecula Jr., Information Security Administrator of the U.S. Geological Survey[8] there are many problems with a requirements analysis. These include:

a. The sponsoring organization may have to make a large commitment in resources.

b. Lack of confidence in the outputs of risk analysis as it is difficult to measure and quantify computer security.

c. There is a question as to which analysis method (and to what depth) is appropriate for any given environment.

d. It is difficult to apply objective measures to subjective judgements.

e. It is difficult to validate inputs and make results consistent.

An example of an informal, non-computerized, risk analysis which can be performed by the end user is the DTNSRDC ADP Security Survey which is based on OPNAVINST 5239.1A. It is listed in Appendix G.

## The Approach

The OISSO must work with each project manager, each DBA, and the end users to determine the following:

- -What assets are to be protected
- -Their value
- -Accessability to these assets, including the question of which of these assets are shared
- -The nature, probability, and rate of various threats
- -Cost-effective responses to those threats
- -Who will be the custodian for both the hardware and each sensitive program and data set.

The OISSO must review these tasks on a regular basis, say yearly, as projects change, new hardware and software are brought in, employees leave, and technology changes.

## The Threats

The threats can be divided between unintentional occurrences and intentional acts of varying degrees of malice. Specifically, they may be broken down as follows:

Unintentional occurrences:

- -Natural disasters such as fire and water damage
- -Electric power line anomalies
- -Destruction of data as a result of reformatting a disk, "wildcard" deletion, copying a file to one which already exists, or improperly using software
- -Modification of data and data integrity problems as a result of improper use of software
- -Disclosure of data

Intentional acts of malice:

- -Hardware and software theft
- -Destruction of data
- -Modification of data
- -Disclosure and theft of data

## The Responses

When deciding on safeguards for PCs, the first question to ask is whether or not the machine is shared. If not, physical access control such as a lock on the PC power switch (as described in the section on "Physical Access Control and Hardware Theft Protection") combined with locking up diskettes or removable disk cartridges with sensitive data may be adequate.

If the PC is to be shared, but data are not, the best solution is to keep sensitive data off the fixed disk and again use only diskettes or removable disk cartridges and combine it with adequate physical area control (as described in the section on "Physical Access Control and Hardware Theft Protection").

If the PC and sensitive data residing on its fixed disk must be shared, one approach that might be taken is to encrypt the data. However, encrypted data can still be deleted and, as Zimmerman states "...the (OISSO) must first ensure the encryption process never writes unencrypted text on hard disk, either through its own procedures or at the option of the user, a condition that rarely will be satisfied." This is discussed further in the section on "Encryption". A second approach is described by Steinauer[9]:

"If equipment must be available for use by many people and cannot be monitored at all times, then hardware or software based security mechanisms should be considered. Such mechanisms can limit the type of access available to each user. This can range from limitations on the files which can be accessed to complete denial of system access. It is possible to set up very restricted application environments which will control the activities of all but the most determined of users. Special menu-oriented software and programs which execute automatically at system start-up can be combined to provide such an environment."

In general, hardware based systems will be more secure than software only systems but the hardware costs more. This is discussed further in the sections on "Logical Access Control". In order for this approach to be effective, the system unit must be physically secured so that there is no access to any circuit boards.

## DISASTER RECOVERY

### Contingency Plan

Any information security system should include a disaster recovery scheme. The OISSO must initiate and monitor this as most users are either unaware of the potential problems or may simply not be willing to spend the time necessary to do it. The DTNSRDC PC contingency plan is listed in Appendix H. A contingency plan should be revised at least annually, store off-site the items listed below in a., b., and c. and enact the following:

a. Maintain records of hardware and software configurations including serial numbers and version or release numbers.

b. Identify time-critical hardware, software, and data within those resources. Any hardware or software which is used on a daily or at least regular basis probably qualifies.

c. Identify temporary alternate computing resources. Consider:
- -Prearranged, off-hour use of PCs from other organizations or departments as part of a reciprocal agreement.
- -Hot site contract if using super-mini or mainframe systems or require extensive networking. An excellent discussion of the topic is offered by Schlosberg[10].
- -Purchase 10% extra hardware above day-to-day needs to be stored off-site, possibly at employees' homes. Hardware might include:
    a. (trans)portable PC with fixed disk
    b. modem
    c. printer
    d. power line conditioner

  [Note that this procedure also helps to eliminate "repair panic" thus reducing maintenance costs for rush jobs.]

d. Identify vendors that specialize in disaster recovery cleanup.

e. Test the plan, at least once a year, using the backed up data, to eliminate surprises.

f. Establish a software backup policy as described below:

### Program and Data Archiving

Program and data archiving on a mainframe system is a normal part of the daily or weekly routine. Users are, to a degree, protected from themselves. Not so on a PC. If the PC is not on a network, the end-user must perform this task. When a PC is shared, an individual must be assigned this task by management. Management must also ensure that all PCs being purchased include some form of backup facility. Consider the following methods:

a. Software controlled backup to floppy diskettes.
This is the least expensive method and can be used on existing PCs. However, the end-user should be warned to NEVER

use the facilities that come with PC-DOS. Aside from being so slow that most people won't use it and having inadequate data compression, there have been reports that the bugs which existed in the PC-DOS 2.1 versions of BACKUP and RESTORE have not been eliminated from PC-DOS 3.1. The user should also NEVER use the PC-DOS RECOVER command to recover lost files. This command can scramble your fixed disk.

A good backup program can back up a 20 megabyte disk onto 45-50 diskettes in less than 30 minutes. Some examples are listed in the section on "Products; Program and Data Archiving and Recovery - Software".

b. Backup to tape cartridges.

This method is a bit more expensive than the first solution. There are two ways to back up a fixed disk to tape. The first is a file-by-file copy. This allows individual file recovery. The second method is called streaming. It is much faster since a mirror image of the disk is dumped onto the tape, however, recovery means reloading the entire disk thus increasing the possibility of file corruption. Some examples are listed in the section on "Products; Program and Data Archiving and Recovery - Streaming Tape Units".

c. Removable Disk Cartridge Units.

This is the most expensive solution, however, it is the most flexible. A dual drive (2 * 20 megabytes) unit costs approximately $2500.00. The time to back up a 20 megabyte cartridge is six minutes on some models. Access time is almost as good as that of fixed disks designed for the IBM PC/AT. Also, cartridges containing sensitive data can be stored in a safe. Since large procurements must be competitive and functionally driven, specifications for a dual drive, removable disk cartridge system are listed in the next section.

It is unfortunate that many people don't back up their data until they have learned that:

- -Fixed disks don't last forever.
- -Fixed disks can and do get wiped out with improper use of the FORMAT and RECOVER commands.
- -Fixed disks can and do get wiped out when using unverified software downloaded from an electronic bulletin board.
- -Fixed disks may not survive a physical move unless the heads have been "parked" in a "landing zone".

Of course, currently active files should be copied to diskette often while the entire fixed disk should be backed up on a regular schedule such as once a month or more. Furthermore, this backup should be stored in a different room or building or in a safe, depending on the sensitivity of the information.

The user should also ensure that all purchased software has been registered and, in the event of say, a fire or flood, attempt to recover the damaged documentation since software companies may require it for replacement.

## Specifications for a Removable Disk Cartridge System

The following is a list of minimum specifications for a dual drive, removable disk cartridge system:

| | |
|---|---|
| Formatted capacity: | 20 MByte/Drive - min. |
| Data transfer rate (best case): | 1.1 MBytes/sec - min. |
| Average access time: | 40 msec. - max. |
| Start/Stop time: | 6/8 sec - max. |
| Power-up time: | 25 sec - max. |
| Time to back up entire disk: (mirror image copy) | 6 minutes - max. (if cartridge capacity exceeds 20 MBytes, max time = capacity/20M) |
| Shock tolerance: | |
| Operating: | 3g - min. |
| Storage: | 40g - min. |
| Vibration tolerance: | |
| Operating (below 17 Hz): | .85g - min. |
| Operating (above 17 Hz): | .25g - min. |
| Storage (below 27 Hz): | 1.3g - min. |
| Storage (above 27 Hz): | 2g - min. |
| Power supply: | Except for host interface adapter (HIU), must have power supply separate from PC. |
| Verification: | Must have post-write verification check. |
| Read/write head protection: | Must have safety mechanism or design characteristic to protect read-write head(s) against "head crashes". |
| Systems Compatibility: | Must interface completely with the IBM PC/XT, IBM PC/AT and strict 100% compatibles. |
| Bootable: | PC must be able to boot up from this system. |
| Operating system: | Must be compatible with PC-DOS 2.1, 3.0, 3.1 and MS-DOS equivalents. |
| Software Compatibility: | Must be able to allow execution of the following software:<br>Lotus 1-2-3 Rel. 2<br>dBase III Plus |

## PHYSICAL ACCESS CONTROL AND HARDWARE THEFT PREVENTION

The OISSO should think of physical access controls as the first line of defense. Some examples of these controls are listed in the section on "Products - Physical Access Control and Hardware Theft Protection." These products fall into the following categories:

a. Area access controls.

Area and room access controls can span a wide range of costs and security levels. They include, but are not limited to:

-Simple door locks.
[Typically, the following controls are used only to protect a mainframe, however, if the situation requires it . . .]
-Card keys using "smartcards".
-Card keys in combination with personal identification numbers (PINs)
-Card keys in combination with biometrics identification such as fingerprints, retina, or voice.

b. System enclosures.

System enclosures are metal cabinets which house the PC system unit and possibly the CRT. They provide both system unit access control and theft protection. They are sold by computer supply catalog houses.

c. Power switch locks.

Although power switch locks are self explanatory, the OISSO should be aware that the IBM PC/AT comes with a cylinder lock which secures both the system and the chassis. Furthermore, it should be noted that devices also exist to lock up the RS-232-C interface thus protecting logical access to serial devices.

d. Lock down devices.

Lock down devices are designed solely for theft prevention and provide no protection from accessing the system. They are generally inexpensive and consist of a vinyl coated steel cable connecting a metal plate to either a second metal plate or a metal fixture which is installed inside the system unit. The metal plate(s) are then glued to the table and system unit.

e. Movement sensors.

Movement sensors quite often are combined with lock down devices and have the same limited function.

f. Data Line Protection.

Devices exist to protect the cable conduit. This is done by wrapping a sensor cable around the transmitting cable conduit. Any tampering with the lines trips an alarm.

## LOGICAL ACCESS CONTROL

### The Problem

When PCs are located in securely locked private offices with only one user per PC in a stand-alone mode, logical access control (restricted access to the fixed disk) may not be cost-effective. Users should consider not storing sensitive information on the fixed disk. Sensitive files should be stored on specially labelled or colored diskettes or cartridges which can be placed in a safe. If users must keep sensitive data on the fixed disk, they should either use a logical access control device, as described in the next section, or encrypt it onto the fixed disk. Encryption is discussed in the sections on On-line and Off-Line Encryption. Encrypted data can still be easily lost, however, and this situation is discussed in the section on Using DOS. There is another alternative which may be adequate for some situations. There are several public domain (freeware or non-commercial software) programs which will "hide" a file or subdirectory from the unsophisticated user.

When PCs are being shared, but the data are not, a bootable, removable disk cartridge unit for about $2500 should be considered. This allows users to "customize" a shared system for individual needs. Functional specifications are included in the section on "Disaster Recovery."

When PCs (and possibly the data residing on the fixed disk) are being shared in an open environment, logical access control may be necessary. Typically, software-only controls range between $40 and $300 and hardware based controls range between $130 and $12,500. Security specialists feel that software-only controls can be defeated more easily than hardware-based controls for the reasons mentioned in the section on NCSC PC Security Perspectives. Hardware-based controls, in the form of adapter boards for the PC, can only be effective, however, if access to the system unit has been secured.

### Logical Access Control Selection Criteria

Logical access control is the process of restricting access to information on the fixed disk. Restrictions can be by file, subdirectory, disk partition, logical disk unit. These restrictions can be for single users or sets of users such as "all members of project XYZ or Code 1234." Some devices, usually hardware, restrict only the ability to boot up the system after either keylock or smartcard is used or after receiving a password. After system entry, these devices provide no further protection.

The following list is an aggregate of the features available in various logical access control products. They are listed loosely in the order of their importance (at least in this author's opinion) although differing circumstances would cause a resequencing.

a. Hardware only vs. software only vs. combination:

Usually, hardware devices will come with at least some software control. Also, as mentioned previously, hardware devices generally cost more than software-only devices, are faster, and provide better security as they are able to prevent boot-up if not provided with the proper password, smartcard, keylock, etc. Of course, the system unit must then be physically secured from unauthorized entry. Software-only controls tend to have more flexibility and convenience features such as more sophisticated menuing, file and subdirectory access, and definition of user groups for selective data access. As described in the sections on NCSC PC Security Perspective and Using DOS, software controls suffer due to the security related inadequacies of DOS and the Intel 8088 and 8086 CPUs.

b. Denial of access to the hard disk upon a floppy diskette boot:

Some devices will allow unauthorized users to use the PC as a floppy diskette-only machine. If an unauthorized user attempts to switch to the fixed disk, the PC responds as if the fixed disk did not exist. Typically, this is a feature of hardware-based devices although some software packages such as Watchdog also have this feature.

c. Password control:

Passwords and encryption keys are the first "line of defense" for almost all logical access control devices known to this author. The OISSO should be aware that sophisticated password control creates a trade-off between ease of use and system protection. If several passwords are required, a system administrator would have to keep track of them and users would probably end up also recording them or shy away from the system altogether. Password management is discussed in the next section. The following list is an aggregate of the types of password control available:

-Minimum and maximum length. Some devices require a minimum number characters for passwords. Also, some devices allow over sixteen characters if desired.
-System access level control. See Section d. below.
-Type of file access permission. See Section f. below.
-One time only guest passwords
-User and project IDs. This can be used for both auditing and defining sets of user groups.
-Character types allowed. Will the device allow use of ASCII characters 128 through 255 ?
-Passwords should be stored in encrypted form.
-Entire password table NOT brought into memory in unencrypted form. Some devices violate this rule to reduce overhead time.

d. System access permission levels:

Some devices provide access restriction at the disk volume, partition, subdirectory, file group, and single file levels. Typically, this is feature of software-only devices. Some packages allow the creation of hidden "disk drives". That is, a logical "D:" drive would be added to the physical C: drive and could only be accessed with the correct password.

e. Automatic file encryption and decryption:

Although this may appear to be merely a convenience feature, it prevents files from inadvertently being stored on the fixed disk in unencrypted form. As described in the section on Using DOS, deleted files may still be recoverable.

f. File access permission types:

Read-only, write-only, file create, delete, modify, etc. This is usually a feature of software-only devices. This is a valuable feature if several people are using a PC for unrelated projects.

g. Encryption speed for 100K byte file:

Typically, hardware encryption is faster than software. However, there are some exceptions to that rule such as Watchdog.

h. Drive lock:

This mechanism prevents fixed disk to floppy disk file copying.

i. Audit trail:

An audit trail is a history of security related events. This history might include events such as logon attempts and times and file or system resource access requests.

j. Menu driven operation and control of access to DOS:

Some of the software-only devices will allow a system administrator to create a menu "shell". This shell allows authorized users to execute only those functions listed in their menu, possibly with an optional permission to exit to DOS.

k. Restricted access to subdirectories created prior to installation of the security device:

Some of the software-only devices will control access only to subdirectories created after installation of that device. They may still control access to the hard disk as a whole, however.

l. Keyboard lock:

A keyboard lock prevents the keyboard buffer from accepting keystroked information. This is useful at lunchtimes, etc. Typically, hardware will provide a more secure keyboard lock than software. For example, a simple, soft reboot will override the keyboard lock in Borland's SuperKey program.

m. Private mailbox:

This allows users to send confidential messages to other authorized users of the system.

Password Management

All PC-based logical access devices known to this author require a password for entry. Some of the password features, listed in the previous section, are discussed below. Some of those features are not found in these devices and as a result, require password management by the OISSO or system administrator (SA). The OISSO or SA should address the following:

a. Password length:
Many of these devices allow as little as one character. Passwords should be at least 8 characters long.

b. Password types:
Since PC-based devices generally do not provide automatic generation of passwords, the OISSO or SA must intervene. Passwords should include nonalphabetic characters and/or according to Goldstein,[11] consist of "nonsense words that are pronounceable so as to be easy to remember but still unusual enough to be difficult for outsiders to guess." An alternative might be to use an acrostic such as "TQBF..." from "the quick brown fox ...". Possibly, the OISSO or SA could provide a set of passwords from which a user could chose.

c. Automatic password changes:
PC based devices do not insist on new passwords after a fixed period of time. Again, the OISSO or SA should intervene to ensure that passwords are changed every three months or less and whenever a user leaves the department. Passwords should also be changed when a PC is sent out for maintenance.

d. Guest passwords:
Unfortunately, only a few logical access devices provide for single use passwords. If a user has no alternative but to allow access to a guest user, s/he should change the password immediately prior to access so that s/he will be reminded to switch back.

e. Multiple password levels:
Many devices allow for multiple password levels and even require separate passwords to access different subdirectories. Unfortunately, if a system becomes too onerous, there will be a tendency for users to record their passwords.

f. Authentication:
Although OISSOs are not likely to control PC access with extraordinary methods such as biometrics, they should look for devices which at least require user and/or project IDs.

g. Automated logons:
Quite often, PCs are used to access other systems. The better communications packages allow the user to create keystroke macros and "scripts" thus enabling a totally automated login. The OISSO should monitor this situation to ensure that passwords are not stored in either keystroke macros or scripts.

h. Lock the "backdoor":
Networks and multi-user systems quite often are delivered with standard passwords for "backdoor" entry by the SA. These passwords should be replaced or removed.

i. Password auditing:
Although PC based devices do not require scheduled password changes as mentioned earlier, some PC LANs such as Novell do. Furthermore, Novell's LAN also keeps a record of the last eight passwords used, which cannot be reused.

i. Device response:
OISSOs should look for devices which lock up after a few incorrect tries and do not respond at all to an invalid password. According to Goldstein,

> "The most important characteristic of system password protection is deadly silence: The system offers the user no information at all until the correct password has been entered; there may then a be system message. There is no prompt or echo of what the user has keyed in: The user can repeatedly enter an incorrect password and the system won't respond. Unless an unauthorized user knows that a system password is required, he might assume that the system is malfunctioning . . ."

Users must also do their part. The users have a responsibility to follow common sense procedures such as:

a. Don't write the password down or keep a copy of the full logon sequence near the computer.

b. Don't use an easily guessed password such as a family name, address or birthday.

c. Don't use the same password on different computer systems.

d. Many systems will indicate the date and time of the user's most recent logout as part of the logon sequence. The user should note that information and contact the OISSO if there are any discrepancies.

Using DOS

The purpose of this section is to provide some "security-related" tips for the novice user of MS-DOS and PC-DOS. Since this author is still hearing reports of bugs in DOS 3.3, it will be assumed that the reader is using version 2.1, 2.11, 3.0, 3.1 or 3.2.

a. Fixed disk organization. Do not allow the root directory to fill up with files. For example, place all DOS command files in the \DOS subdirectory, all batch files (except AUTOEXEC.BAT) in the \BATCH subdirectory and all utilities in the \UTIL subdirectory. The following path statement, placed in the AUTOEXEC.BAT file, will tell the command processor where to look for DOS commands, batch processes, and utilities:

```
PATH C:\;C:\DOS;C:\BATCH;C:\UTIL
```

b. Accidental formatting of the fixed disk. The user can prevent this by doing the following:

1. Rename the DOS FORMAT.COM file to XFORMAT.COM

2. Create a batch file called FORMAT.BAT to include:

```
CD\DOS
XFORMAT A:
CD\
```

The user should also be aware that when using some combinations of memory-resident software (such as SuperKey and Sidekick) with certain disk controllers, the format function may not work at all.

c. The user should be aware that deleting a file, by using either ERASE or DEL does not actually get rid of the file. The disk clusters which hold the data have been freed but not wiped clear and the disk directory still contains the file name except that the first character has been replaced with a hexadecimal character "E5". This is why file recovery programs such as the Norton Utilities can be effective although even they may not work if there has been subsequent output to that disk. The user then must be careful not to give other users a diskette which contains deleted files of sensitive data. If the user does indeed wish to destroy the contents of a file, the Norton Utilities contain programs to wipe both files and complete disks clear.

d. Memory residue. The user should be aware that after a program is finished, sensitive data may still reside in memory. A soft reboot (ctrl - alt - del) should clear user addressable memory but the user should confirm this with the manufacturer of the PC. (A soft reboot may not clear the I/O buffers and hence is not adequate for TEMPEST concerns).

e. File copying. DOS files are copied by sectors. As a result, data from a previous file may be inadvertently transferred to another file. Although time consuming, the best assurance is to compare source and target files using the DOS command COMP. Also, the user may wish to set VERIFY = ON in the AUTOEXEC.BAT file to instruct DOS to verify that sectors written on the target media are recorded properly. The user is further reminded that a COPY does not affect the source file but will delete an existing file in the target subdirectory if it has the same name as the target file.

f. File and subdirectory attributes. The user can prevent accidental erasure or modification of a valuable file by modifying the attributes of that file. This can be done by using the PC-DOS 3.x ATTRIB command. ATTRIB can switch a file between "read-only" and "normal" but will not prevent data loss if the media is reformatted. A freeware utility called ALTER can switch the read-only, hidden, system, and archive attributes for both DOS 2.x and 3.x files. This utility can be downloaded from many electronic bulletin boards.File and subdirectory attributes are described by a single byte (#11) in each file's directory entry. These attributes include:

- Read-only file. The file is included in a normal directory search and can be copied but not deleted.

- Hidden file. The file is excluded from a normal directory search, and cannot be deleted or copied. This attribute can also be assigned to subdirectories. A user may still transfer to a hidden subdirectory using "CD\subdirname". Also, many freeware directory sort routines, along with the Norton Utilities do not "play by the rules" and will display hidden subdirectories and files.

- System file. The file is excluded from a normal directory search, and cannot be deleted or copied. However, many freeware directory sort routines, along with the Norton Utilities do not "play by the rules" and will display system files.

- Reserved for DOS.

- Subdirectory. This entry is a subdirectory. As described above, it can also have the "hidden" attribute and in such a case will not appear when a DIR command is invoked.

- Normal file. This is not a separate attribute. It simply means "none of the above".

- Archive bit. It is used by BACKUP and RESTORE to determine whether or not a file has been archived.

- Reserved for DOS.

## Off-Line Encryption

Encryption can be an effective means for restricting file access although these files can still be easily deleted. The best known encryption technique is the Data Encryption Standard or DES, developed by IBM for the National Bureau of Standards (NBS). Although DES is about ten years old, it is still considered quite adequate for unclassified information.

There are dozens of encryption devices available. The hardware devices are much more expensive than the software-only devices but generally are faster and more secure. Another choice which must be made is whether to use a "private key" system such as DES or a "public key" system (PKS). In a private key system, the encrypting and decrypting keys are the same, thus requiring the sender to give the receiver the key value. In a public key system, the receiver has a private decryption key and anyone wishing to send him secure information need only look up his public encryption key. Off-line encryption is that which is performed on local disk files. It is usually software-based and uses a private key system. On-line encryption means encrypting "on-the-fly" and will be discussed in the section on "Communication Security."

When selecting an Off-line encryption device, the following features should be considered:

a. Hardware only vs. software only vs. combination:
Generally, hardware-based encryption is more secure since software can be more easily reverse-engineered. It is also usually faster but more expensive. Most off-line encryption devices are software-only, whereas on-line encryptors are always hardware-based. In some cases, on-line encryptors include off-line encryption as an option (in which case, it is called pre-transmission encryption).

b. Interface type:
If it is a hardware device, does it require an expansion slot? A device will be more secure if it can be physically secured inside the system unit. If it requires an expansion slot, does it use (or share) a direct memory access (DMA) channel or a serial (COM port), parallel (LPT port), or reserved interrupt? This is important as there are not many channels or hardware interrupts available. Also, if the PC is an IBM clone, the device should be tested on that machine before purchase.

c. Encryption algorithm:
Does the device use DES or a proprietary algorithm? Generally, proprietary algorithms take less time but are considered to be less secure. DES is a private key system. If DES is not used, does the algorithm use a private key or public key scheme such as RSA?[12] Public key schemes are discussed further in the section on Network Access Control and On-Line Encryption Devices.

d. Encryption speed:

Devices are usually rated on the time required to encrypt a 100 kbyte file. This can range anywhere from less than one second to 4-5 minutes. A survey of data encryption devices by PC Week[13] includes encryption speeds for 40 devices.

e. NBS certification:

Several products claim to be NBS certified. In some cases, this is deceptive. NBS does not certify any software and the only hardware which NBS will certify is the microchip which performs DES encryption/decryption. NBS does not certify the entire product. Although the DES algorithm is NBS certified, a vendor's use of that scheme does not automatically infer product certification.

f. Automatic encryption on file save:

Some devices keep the encryption/decryption process transparent to the user. This prevents cleartext from being accidentally written to the disk.

g. Encrypted file format:

Some devices offer a choice of ASCII and non-ASCII output from the encryptor. This can be helpful when transmitting encrypted files over some networks since some non-ASCII characters may either be stripped from the file or interfere with network operation.

h. Auto-purge or auto-delete of the source file:

Some devices will automatically overwrite the cleartext source file during the encryption process.

i. Group file encryption:

Some devices allow files to be grouped together for mass encryption on a single encryption key. This may be by named list or by entire subdirectory.

j. Master key for system administrator or OISSO:

Some devices leave a "back door" open so that a system administrator can decrypt any file on the system.

k. Overhead:

If there is a one-to-one translation of cleartext into ciphertext, encrypted files can occupy the original disk space.

Devices which encrypt data for transmission have additional features and will be listed in the section on "Communications Security - Network Access Control and On-Line Encryption."

## The Problem

Whenever PCs are connected to a host via a line which is not secure, the OISSO has three primary security related concerns:

-Ensuring that the received sensitive data actually:
  (1) arrived from its stated source, and
  (2) arrived unmodified.
-Ensuring that sensitive data are not disclosed.
-Ensuring that only authorized users can access the host.

The first concern is resolved if the product strictly adheres to DES since DES includes provision for authentication of the received data. On-line encryption devices are usually sufficient to satisfy the second concern and security modems will keep out all but the most determined of individuals. Network access control systems deal with all three problems, however, they usually do not include the modem and may employ encryption only as an extra option.

## Network Access Control and On-Line Encryption Devices

On-line encryption can be an effective means for ensuring that communications are kept private. These devices would be placed between the modem and host, front-end processor, PC, or terminal. In determining which products to select, the OISSO must consider all the features mentioned under Off-line encryption devices plus some additional ones. First, let us return to the issue of public (PKS) versus private key techniques as it takes on more significance in a communications environment. According to ACS[14], PKS systems can be spoofed:

"Let us presume that our data thief (legitimately!) buys the same PKS equipment as our Users A and B, who both use dial access. Our thief, T, powers up his PKS device, dials User A, and sends to A his public encryption key $E_T$ but identifies himself as User B. User A thinks he has received $E_B$, generates a working key $W_{AB}$ for the A/B session, encrypts $W_{AB}$ with $E_B$ (really $E_T$), and sends it to B (really T). Thief T uses [decryption key] $D_T$ to obtain $W_{AB}$ and now may securely talk to User A. A has been spoofed!"

Although this is a very sophisticated attack requiring some expensive equipment and precise timing and might be solved by placing $E_B$ in a public directory, at least some security experts consider that this is not a contrived situation.

When selecting a network access control system or an on-line encryption device, the following features should be considered in addition to those listed under off-line devices:

1. Fail-Safe operation:
   This is achieved with internal circuitry monitoring the encryption operation. If a problem is detected, the device should either shut down or set an alarm.

m. GSA Federal Standard FS 1027:
Devices which adhere to this standard must:
- Use DES.
- Transmit only ciphertext.
- Be securely installed to prevent unauthorized access.
- Generate an alarm if an intrusion is detected.
- Have a failsafe provision to prevent interruption of the encryption process.
- Use manual key entry.
- Not disclose its key variables.

n. Encryption approach:
Is the device protocol-sensitive (end-to-end encryption), protocol-independent (transparent or link encryption), or both? Protocol-sensitive devices will not generate output that is "protocol-like" and hence confuse an intelligent multiplexer. Also, communications resources are more efficiently used by protocol-sensitive devices.

o. Character Output:
Does the device generate special control characters as part of the encrypted message or only those control codes consisting of the standard characters necessary for error correction and handshaking? Special characters might interfere with some communications networks.

p. Message authentication:
A device with this feature can determine whether a message has been altered during transmission and whether it came from its stated source. DES incorporates message authentication.

q. Cleartext operation:
This option allows the device to communicate with other terminals and hosts which do not use encryption.

r. Voice encryption:
Some devices will encrypt and transport digitized voice signals.

s. Key generation unit:
These devices are portable and plug into the encryption device. They must be manually transported to the encryption device at the other end to allow data transmission.

t. Pre-transmission encryption:
Some on-line encryptors optionally allow off-line encryption for protection of files stored locally on disk.

The following are pertinent transmission characteristics:

u. Configuration:
Most devices communicate only from point-to-point (single site to single site) whereas some will operate in a multipoint configuration (host to terminals).

v. Synchronization:
Most devices allow both synchronous and asynchronous operation. Typically, synchronous mode is used for higher speed transmissions.

w. Transmission modes allowed:
Almost all of the devices support full duplex (bi-directional) transmission while most include half duplex (one direction at a time). Simplex (one direction only) transmission is not well supported as it is not as commonly used.

x. Data rates supported:
Typically, most devices will handle transmission rates between 300 bits per second (bps) and 19.2 Kbps. At least one device, by Cylink, will transmit up to 7 Mbps.

y. Modem compatibility:
Does the device recognize the Hayes Command set?

The following are additional controls to look for in a network access control system:

aa. Audit trail:
The purpose of an audit trail is to record the security-relevant events on the system. This should include:
- Date and time of all access attempts.
- User ID.
- Password used.
- Number of attempts (if more than one, passwords used).
- Disconnect time and/or duration of connection.
- Which line the call came in on.
- Violation type (if any). As most access attempts do not result in violations, this might best be highlighted by being placed in a separate file and cross-referenced to the previously listed items. As described in the Datapro Report on Information Security, a sophisticated network access control device such as Avant-Garde's Net/Guard 3 car generate audit reports by user, session, hour of the day, this day, yesterday, week-to-date, previous week or month, month-to-date plus customized reports. It reports (and either refuses access or automatically disconnects) on violations such as those listed below:

ab. Disconnect controls and alerts:
- Attempted logon with an invalid or inactive password.
- Attempted logon with a duplicate or unauthorized ID.
- Time of day or day of week restriction.
- Idle time exceeded.
- Percentage of lines available for group usage exceeded.
- Maximum number of days without password change exceeded.
- Total daily or session connect time exceeded.
- Number of logon attempts exceeded.
- Rate of logon attempts exceeded.
  [Restricting access attempts to, say, one per 30-60 seconds makes it very time consuming for hackers to sequence through ID/password combinations.]

ac. Port camouflage:

Some of the network access devices operate on the analog side of the modem but more operate on the digital side. If the device operates on the digital side of the modem, does it prompt the user? No prompt at all is best. If the device operates on the analog side of the modem, can it mask the modem tone from the caller. This is an important feature as it provides a lower operating cost alternative to the callback modem. On the other hand, this can be difficult for legitimate callers if the modem is not within hearing range. Some devices respond with a synthesized voice (instead of a modem tone) requesting an entry code.

ad. Security handshaking modes:

(1) Encryption.

(2) Password/Callback. Although callback usually is to a fixed location, some of the more sophisticated can dynamically reprogram user configurations to allow alternate and mobile location callback numbers. This is discussed further in the section on Security Modems.

(3) Random password generation (RPG). A unique "session" password is generated by a hand held "calculator" type device issued to authorized users in response to a random challenge from the access control device.

(4) Automatic algorithm comparison. A "key" is used to automatically generate a verification dialogue. Any of the following "keys" might be used:
- Single user physical key.
- Smart Cards. Some systems can actually use an individual's own credit cards!
- Biometrics. Fingerprints, retina, voice, or signature.

ac. Intruder alarm:

This can be audible and/or visual.

ad. Number of ports protected:

This is the number of incoming calls the device can handle simultaneously. Some devices, such as the Avant-Garde Net/Guard 3, can handle up to 4096 ports at a time.

ae. Number of user access codes allowed:

This is the number of password combinations allowed. This is determined by the maximum password length and the number of special characters allowed. Some devices allow up to $(36)^{96}$ combinations.

af. Access by user group:

Some devices restrict access to specific applications as determined by user group.

Security Modems

The purpose of a security modem is to provide relatively inexpensive, single-line access control for a small host computer. These modems employ one or more of the following schemes: encryption, password protection, and callback operation. Some features to look for in security modems:

a. Audit trail (as described in the previous section).
b. Battery backup or nonvolatile memory.
c. Network controls such as auto logon to specific applications.
d. Callback on a second, "private" line.

The operations of encryption and password modems are self-explanatory. Callback modems operate as follows:

- The device is initialized with a list of authorized users, their access code(s), and their phone number.

- The remote user calls the host.

- The callback device requests the access code which is then supplied by the user.

- The callback device disconnects the user, then compares the incoming access code against the stored list. If there is no match, the device does nothing. If there is a match, the device calls the user back at the phone number which corresponds to the access code. Some devices call back on the same phone line while others have the option of calling back on a second "private" line.

The advantages of using this type of access control are:

a. If the host site is willing to pay for the outgoing calls, the cost of a WATS line would be less than the aggregate charges incurred by individual users.

b. Security modems do not cost much more than ordinary intelligent modems and eliminate the need for a stand-alone, network access control device. This simplifies network configuration, installation, and maintenance.

There are some disadvantages however:

a. Encryption-based modems would probably have to be purchased in pairs.

b. Callback modems would not allow convenient access to authorized users who travel.

c. Callback operation can be circumvented by call-forwarding.

d. Many System Administrators do not want to incur the cost for all of the phone calls.

NETWORK SECURITY

Network Management Policy

In order to provide network-wide security, management must address five main issues. They are physical access control, logical access control, encryption, message authentication, and auditing. These issues should be an integral part of the initial configuration design.

Physical Access Control

Physical access control for the network as a whole can be enhanced in a few ways. They include the following:

a. Cabling. As mentioned previously, devices exist to protect the cable conduit.

b. Console-less server. One means of limiting access to the network server is to eliminate the keyboard and video display from the server. For example, 3Com uses an AT clone so configured.

c. Diskless PCs. There is a new class of PC available. They are designed specifically for use on a LAN.[15] They are true PCs except that they have neither floppy nor fixed disks included. These PCs range in price from $699 to $3000 and have a strong security advantage. Users can neither steal software from the network nor load any unauthorized programs onto the network.

Logical Access Control

Logical access control to the network as a whole is usually provided by a network access device as described in the section on Communications Security, however, the network operating system (NOS) or multi-user operating system (MOS) must have additional controls to protect itself and specific resources such as files, printers, or modems. The following security features should be considered:

a. Login facilities. Network access can be controlled in the following ways:
- User ID and password
- User classification and level (administrator, server user, user, and member of user group)
- Physical volume, logical disk partition, directory, file groups, and files.
- Resource (servers, printers, plotters, modems, etc.)
- Access rights/privileges.

Note that many LAN hardware adapters have built in IDs for further access control.

b. Persistent Naming. Persistent naming means users have permanent network names. Without persistent naming, there can be no user profiles, rendering login and audit controls ineffective.

c. Keyboard Locking. Some networks allow operation with the keyboard locked.

d. Access level. There can be several levels of access rights to a volume, directory, file, or record. They include:

- Read
- Write
- Read/Write
- Read/Write/Create
- Write/Create/Noread
- Delete
- Search (directory)
- Private: Read/Write/Create/Exclusive
- Public: Read
- Shared: Read/Write/Create
- Parental rights (giving authorized users the right to grant access rights to other users

Encryption

Encryption is essential to the protection of information on a LAN. On-line encryption is more suited for a LAN than off-line encryption since it is transparent to the user and as it is hardware, is faster and more secure. On-line encryption is described in the section on Communications Security. As described in that section, there are two approaches: end-to-end (protocol-sensitive) and link (protocol-independent) encryption. Some devices will allow either approach.

Message Authentication

An important aspect of message transmission is the authentication of the transmitted packets. This means that the receiver should be able to verify that the packets have not been corrupted and that they did indeed come from the stated sender. Also, the sender should be able to verify reception. Message authentication is an integral part of DES.

Auditing

The network should maintain an audit trail of security-relevant events. In the section on Network Access Control, the audit trail for entry to the system as a whole is discussed. In addition, the NOS/MOS should maintain a history of requests for specific resources such as servers, printers, plotters, modems, etc. and data at the physical volume, logical disk partition, directory, file group, and file levels.

For additional security, when a user logs to the system, it should display the date and time of the most recent login. This will alert the user to any unauthorized use of his password.

Many of the features listed here are incorporated into the Novell, 3Com, Unix, Xenix, QNX, and other operating systems.

DATA BASE SECURITY

Overview

Multi-user data base security issues are quite similar to network security issues. In fact, for any kind of effective data base security (particularly, record locking), the DBMS must work in concert with the operating system. Briefly, the issues are:

-User profile
* identification (user name)
* authentication (confirm stated user's identity)
* association (user is a member of one or more authorized groups such as personnel or accounting)
* accountability (individual users can be made responsible for the security and integrity of data down to the data element level if necessary.)

-User/Group authority with respect to:
* Accessible objects (e.g. accounting users may access only financial data)
* Allowable operations (e.g. accounting users may run only accounting programs)

[A list of allowable operations can be found in the section on Network Security, 2.c, Access Level.]

-DBMS controls
* Encryption of programs and database (should be automatic)
* Internal audit (historical record of user requests)

An Example

dBASE III Plus appears to be an excellent example of data base security for a small, PC-based, multi-user data base system. dBASE III Plus addresses all of the above mentioned issues except internal auditing. This system will work in either a stand-alone or LAN environment. A DBA is required to orchestrate the controls such as assigning users to groups and assigning access levels.

dBASE III Plus offers three types of security:

1. Controlled access to dBASE
This is accomplished by setting up a user profile which includes:
- Login name
- Password
- Group name (the user may be a member of several groups)
- User access level (used the with file operation privilege level to determine actual user rights)
- Account name (this is not used for authentication but to provide additional project information)

2. Controlled access levels to:
   - Data files
   - Fields in the data base
   - Application program code

   [dBASE III Plus does not provide access control at the record level, however, this is not necessarily unreasonable for a relational data base.]

   File access privileges include:
   - Append new records to a database file
   - Delete records from a database file
   - Read records from a database file
   - Modify record contents in a database file

   There are eight access levels for each of the above mentioned privileges.

   Field access privileges include:
   - Read and write the field
   - Read but not write the field
   - No access

   There are eight access levels for each field in the database file.

3. Data file and program encryption
   - Encryption and decryption are automatic
   - Encryption/Decryption keys are unique to each group

ELECTRICAL POWER LINE PROTECTION

The Problem

Electrical power line anomalies can damage a PC, cause loss of data, or at the very least, force the machine to reset and reboot. The problems include the following:

a. Voltage surges and transients.

A voltage surge is a rise in voltage that exceeds a thousandth of a second. Typically, they may reach a few hundred volts for one or two cycles.

b. Voltage spikes

Voltage spikes usually last less than a thousandth of a second and can exceed several thousand volts. The best known cause is lightning.

c. Noise

Noise is high frequency (and sometimes high voltage) interference on the power line. The two main causes are electromagnetic interference (EMI) from motors, typewriters etc. and radio frequency interference (RFI) from radio, TV, microwave transmitters etc. There are two types of noise: transverse-mode (hot line - neutral) and common-mode (hot line - ground). They can cause low level timing and logic errors resulting in lost or corrupted data. The two types of noise may require different solutions.

d. Voltage sags

Voltage sags are brief voltage drops lasting only a few cycles. They are caused by fault clearing devices and large load changes. This situation has occurred at DTNSRDC.

e. Brownouts

Brownouts are voltage reductions (5 - 15%) which occur when the power load exceeds the electric company's power capacity.

f. Power outages or blackouts

Any voltage drop below 85% of normal will appear as a blackout to a PC power supply. If power is allowed to surge back automatically, PC components such as the CPU can be severely stressed.

There are solutions to each of these problems. It should be noted first that surge protectors under about $50 - $60 are probably worthless! Second, use properly grounded outlets, and third, make sure that no other heavy or motorized equipment is connected to the same circuit breaker.

Commercial solutions are listed below:

| | |
|---|---|
| a. Line filter: | transverse-mode noise. |
| b. Surge suppressor: | surges, spikes. |
| High end models: | all modes of noise, modem protection. |
| c. Isolation transformer: | voltage transients, common-mode noise. |
| d. Line conditioner: | all modes of noise, surges, spikes, sags, brownouts. |
| e. SPS and UPS: [Standby and uninterruptible power supply] | all modes of noise, surges, spikes, sags, brownouts, blackouts. |

Typically, the solutions chosen are surge protectors, standby power supplies (SPS), or uninterruptible power supplies (UPS). Below are listed some of the selection criteria for surge protectors, SPSs and small UPSs.

Surge Protection Selection Criteria

Users should be aware that even the protection provided by some of the best surge protectors deteriorates with the number of times it receives severe hits. A good surge protector should meet the following specifications:

a. Response time of 1 nanosecond or less.
b. Energy absorption (transient suppression) rating of 40 Joules or more.
c. Maximum average power dissipation of at least 1.5 kilowatts at 1 millisecond.
d. Maximum transient voltage of at least 6000 volts.
e. Maximum clamping voltage of no more than 340 volts @ 50 amps.
f. Current peak of at least 4500 amps.
g. Test voltage of at least 1750 volts for 1 second.
h. Meet or exceed IEEE 587A and 587B.
i. UL approved.

Many surge suppressors include noise filtering. It should meet the following specifications:

j. Noise rejection frequency (transverse & common modes):
0.5 MHz to 25 MHz attenuated by at least 45dB.

Many surge suppressors include modem surge protection. It should meet the following specifications:

l. Response time of 1 nanosecond or less.
m. Maximum clamping voltage of no more than 350 volts @ 5000 amps
n. Peak breakdown voltage of 225 to 315 volts @ 1 milliamp.
o. Reverse standoff voltage of 256 volts.

Standby and Uninterruptible Power Supply Selection Criteria

The difference between a standby (or backup) power supply (SPS) and an uninterruptible power supply (UPS) is that an UPS is always on-line and an SPS is always off-line. This means that an SPS has to be triggered on and off. This can take a few milliseconds. To the user, this may be critical as the power supplies to some IBM PC/XTs will drop the power-good signal after only a few millisecond lapse. The result is loss of all data in memory and probably an automatic reboot. According to Rosch[16] this problem applies to power supplies made in Mexico by Zenith for IBM.

In any case, the user should understand that the purpose of a small, "PC sized" UPS or SPS is to provide sufficient time (typically 10 -15 minutes) for an orderly shutdown of the PC. Its purpose is not to allow the user to "ride out the storm". Therefore, printers shouldn't be plugged into a UPS or SPS.

A good UPS should meet the following specifications:

a. Power capacity
   -AT class machines: 400 watts minimum.
   -XT class machines: 330 watts minimum.
b. Battery power duration time of at least 10 minutes at full load.
c. Waveform: Sine is preferred over rectangle but is much more expensive.
d. Line conditioning.
e. Separate conditioning for each line (optional).
f. Output voltage after 10 minutes at full load: at least 104 VAC
g. Output frequency variation not to exceed 1% of 60 Hz.
h. Low battery warning.
i. Battery life (and ease of replacement) of at least 3 years.
j. Transient suppression of at least 80 joules.
k. UL approved.

Other features which may be of concern are:

l. Number of outlets.
m. Size and weight.
n. Heat and noise level generated.

The buyer of an SPS must also be concerned about the following specifications:

o. Transfer time of no more than 5 milliseconds.
p. Line synchronization.
q. Low voltage trigger on at approximately 105 VAC.
r. Low voltage trigger off at approximately 109 VAC.

COMMENTS

The user is reminded that the product survey in no way implies an endorsement by the U.S. Navy. Furthermore, this survey is not meant to be a comprehensive listing but instead merely attempts to display a range of products which are available at the time of this writing in order to match the desired level of security with the available resources.

## PROGRAM AND DATA ARCHIVING AND RECOVERY

### Removable Disk Cartridge Units

Bernoulli Box
Iomega Corp. [Gov't & East coast accounts]
3390 Peachtree Road NE, Suite #1000
Atlanta, GA 30326
(404) 261-7815

GenieBox
Genie Technologies Corp. [Iomega OEM]
31117 Via Colinas, Suite #402
Westlake Village, CA 91362
(818) 991-6210

WestWind Computer
1690 65th Street
Emeryville, CA 94608
(800) 526-6500

### Software

Fastback 5.1
Fifth Generation Systems
7942 Picardy Ave.
Baton Rouge, LA 70809
(800) 225-2775

Norton Utilities
Peter Norton
2210 Wilshire Blvd. #186
Santa Monica, CA 90403
(213) 399-3948

ARC [This popular shareware program is also available from many electronic bulletin boards but beware of corrupted copies.]
System Enhancement Associates
21 New Street
Wayne, NJ 07470

## Streaming Tape Units

QIC-60AT/QIC-60H
Tecmar Inc.
6225 Cochran Road
Solon, OH 44139-3377
(216) 349-1009

TG-4060/1020i/1020e
Tallgrass Technologies
11100 W. 82nd Street
Overland Park, Kan. 66214
(913) 492-6002

Irwin 110/120/145/310
Irwin Magnetics
2311 Green Road
Ann Arbor, Mich. 48105
(313) 996-3300

# PHYSICAL ACCESS CONTROL AND HARDWARE THEFT PREVENTION

## Area Access Control

Cardkey Systems
300 W. Service Road
Herndon, VA 22070
(703) 478-5775

Synergistics Inc.
3 Eire Drive
Natick, MA 01760
(617) 655-1340

Identix Biometric Identification System [Fingerprints]
Identix Inc.
2452 Watson Court
Palo Alto, CA 94303
(415) 858-1001

## System Enclosures

Micro Cabinet
Devoke Data Products
1500 Martin Ave.
Box 58051
Santa Clara, CA 95052-8051
(408) 980-1360

## Power Switch Locks

PC Lok & Keyboard Lok
Devoke Data Products

Terminal Locking Device (TLD)
Black Box Corp.
Mayview Road at Park Drive
Box 12800
Pittsburgh, PA 15241

## Lock Down Devices

ANCHOR PAD
Anchor Pad Security Services
8121 Georgia Ave. #407
(301) 589-7474

THEFT GUARD PC Cable Screwlock
Theft Guard Computerized Mfg. Cons., Inc.
106 Wilmot Road
Deerfield, IL 60015
(312) 940-0010

## Movement Sensors

THEFT GUARD Squealer Alarm
Theft Guard Computerized Mfg. Cons., Inc.

Model 813 Electronic Theft Protector
Terminal Data Corp.
15733 Crabbs Branch Way
Rockville, MD 20855
(301) 921-8282

## Data Line Protection

INFOGARD
GTE Security Systems
P.O. Box 1448
Mountain View, CA 94042
(415) 966-2210

## Software

Protec 3.1
SOPHCO
P.O. Box 7430
Boulder, CO 80306
(303) 444-1542

Knight Data Security Manager
AST Research Inc. [SOPHCO OEM]
2121 Alton Ave.
Irvine, CA 92714
(714) 863-1333

Watchdog
Fischer Innis Systems Corp.
4175 Merchantile Ave.
Naples, FL 33942
(800) 237-4510

TheEMCEE
Command Software Systems, Inc.
31236 Bailard Road
Malibu, CA 90265
(800) 423-9147

SecretDisk
Lattice, Inc.
P.O.Box 3072
Glen Ellyn, IL 60138
(312) 858-2190

SECURE! PS
Winterhalter Inc.
P.O. Box 2180, Dept. P.S.
Ann Arbor, MI 48104
(313) 662-2002

Vfeature
Golden Bow Systems
2870 Fifth Ave., #201
San Diego, CA 92103
(619) 298-9349

## Hardware

X-LOCK 100
A-O Electronics, Inc.
2137 Flintstone Drive
Tucker, GA 30084
(404) 491-8044

ENIGMA
Vutek Systems
10855 Sorrento Valley Road
San Diego, CA 92123
(800) 621-0852 ext. 152

ShurLock Security System
P.C. Holmes Inc.
4605 Post Oak Place Drive, Suite 209
Houston, Texas 77027
(713) 840-7771

Lockit I/Lockit II
Security Microsystems Consultants
16 Flagg Place, Suite 102
Staten Island, NY 10304
(718) 667-1019

CyLock
Cytrol Inc.
4620 West 77th Street
Edina, MN 55435
(612) 835-4884

Distributor:
Business Machine Security, Inc.
230 Park Ave., Suite 1903
New York, NY 10169
(800) 328-0056

Access Control Module
Isolation Systems
26 Six Point Road
Etobicoke, Ontario Canada M8Z 2W9
(416) 231-1248

## Off-Line Encryption Devices

PrivacyPlus
United Software Security Inc.
8133 Leesburg Pike, #800
Vienna, VA 22180
(800) 892-0007

SuperKey
Borland International Inc.
4113 Scotts Valley Drive
Scotts Valley, CA 95066
(408) 438-8400

COMMUNICATIONS SECURITY

## PC/Terminal-to-Host Access Control

EyeDentification Data Base Security System
Eyedentify Inc.
P.O. Box 3827
Portland, OR 97208
(503) 645-6666

TS300 Security System
Time and Data Systems International Ltd.
Crestworth House, Sterte Ave.
Poole, Dorset BH15 2AL, England
(202) 670055

LazerLock
United Software Security Inc.
8133 Leesburg Pike, #800
Vienna, VA 22180
(800) 892-0007

## Network Access Control and On-Line Encryption Devices

Mailsafe [software only]
RSA Data Security, Inc.
10 Twin Dolphin Drive
Redwood City, CA 94065
(415) 595-8782

DataLOCK 4000
MicroFrame, Inc.
2551 Route 130
Cranbury, NJ 08512
(609) 395-7800

MultiSentry/ComputerSentry
Tact Technology
100 North 20th Street
Philadelphia, PA 19103
(215) 569-1300

Sherlock PC/ISM/ISM-Federal
Analytics Communications Systems, Inc.
1820 Michael Faraday Drive
Reston, VA 22090
(703) 471-0892

Datacryptor 64/64-1027
Racal-Milgo, Inc.
1601 North Harrison Parkway
P.O. Box 407044
Sunrise, FL 33340
(305) 475-1601

CRYPTOCOMM II, CRYPTOLOCK II
COMMCRYPT, Inc.
11005 Piney Meetinghouse Road
Rockville, Maryland 20854
(301) 299-7337

GILLAROO, GUARDSMAN
PE Systems, Inc.
5520 Cherokee Avenue
Alexandria, VA 22312
(703) 642-9300

Security Modems

GTX-100
A-O Electronics, Inc.
2137 Flintstone Drive
Tucker, GA 30084
(404) 491-8044

Security Modem
Cermatek Microelectronics, Inc.
1308 Borregas Ave.
Sunnyvale, CA 94086
(408) 752-5000

Oz Guardian 533
Tri-Data Corporation
505 E. Middlefield Road
Mountain View, CA 94043
(415) 969-3700

MD212 Security Plus
Ven-Tel, Inc.
2342 Walsh Ave.
Santa Clara, CA 94043
(408) 727-5721

Zoom/Modem PC 1200 & PC 2400/XL
Zoom Telephonics, Inc.
207 South Street
Boston, MA 02111

NETWORK SOFTWARE

VSLAN
Verdix Inc.
Chantilly, Virginia

NetWare Operating System
Novell, Inc.
748 North 1350 West
Orem, Utah 84057
(801) 226-8202

3+/3+ Share/EtherSeries
3Com Corp.
1365 Shorebird Way
P.O. Box 7390
Mountain View, CA 94039
(415) 961-9602 (301) 921-4390 [U.S. Navy Sales Rep]

QNX
Quantum Software Systems Ltd.
215 Stafford Road
Nepean/Ottawa, Ontario, Canada K2H 9C1
(613) 726-1893

Xenix 3.0
MicroSoft Corp.
10700 Northup Way
P.O. Box 9700
Bellevue, WA 98008
(206) 828-8080

UNIX
AT&T
100 Southgate Parkway, Room 2D-10
Morristown, NJ 07960
(800) 247-1212

USECURE [UNIX software enhancements]
Unitech Software Inc.
8330 Old Courthouse Road, Suite 800
Vienna, VA 22180
(703) 734-9844

ELECTRICAL POWER LINE PROTECTION

## Surge Protection

Masterpiece/Masterpiece Plus
Kensington Microware Ltd.
251 Park Ave. South
New York, NY 10160-9990
(212) 475-5200

Power Director
Computer Accessories Corp.
7696 Formula Place
San Diego, CA 92121
(619)-695-3773

Diamond/Emerald/Ruby/Sapphire
Curtis Mfg. Co., Inc.
305 Union Street
Peterborough, NH 03458
(603) 924-7803

## Standby and Uninterruptible Power Supplies

Micro Ferrups
Best Power Technology, Inc.
P.O. Box 280
Necedah, WI 54646
(608) 565-7200

SPS 400 A/800 A/Mini-UPS
SOLA Electric
1717 Busse Road
Elk Grove Village, IL 60007
(312) 439-2800

SPS 400-A
Safe Power Systems
528 W. 21st Street
Tempe, Ariz. 85282
(602) 894-6864

BC425 FC
Tripp Lite
500 N. Orleans
Chicago, IL 60610
(312) 329-1777

MM 500/1
Para Systems
11425 Mathis Street #404
Dallas, TX 75234
(214) 869-1237

ACKNOWLEDGMENTS

I would like to thank W. Fung, C. Davis, Dr. S. Berkowitz, J. Hays, and P. Marques for their review of this report. Their comments were most helpful.

## Appendix A. BIBLIOGRAPHY

The following is a list of publications by the National Computer Security Center (NCSC). Much of the work done by this NSA organization is directed towards TEMPEST issues and securing classified level information on mainframes, however the reader may find some of these publications of use.


1. DoD Trusted Computer System Evaluation Criteria, (DoD 5200.28-STD), GPO Stock No. 008-000-00418-8. Revised Dec 1985, ["The Orange Book"]. This manual supercedes CSC-STD-001-83, 15 Aug 1983.

2. PC Security Considerations, (NCSC-WA-002-85), GPO Stock No. 008-000-00439-1. Dec 1985, ["The Powder Blue Book"].

3. DoD Password Management Guideline, (CSC-STD-002-85), GPO Stock No. 008-000-00443-9. 12 Apr 1985, ["The Green Book"].

4. Computer Security Requirements - Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments, (CSC-STD-003-85), GPO Stock No. 008-000-00442-1. 25 June 1985, ["The Yellow Book #1"].

5. Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements - Guidance For Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments. (CSC-STD-004-85), GPO Stock No. 008-000-00441-2. 25 June 1985, ["The Yellow Book #2"].

6. DoD Magnetic Remanence Security Guideline, (CSC-STD_005-85), 15 Nov 1985. ["The Blue Book"].

7. Information Security Products and Services Catalogue, Published quarterly.


The following is a list some of the security-related publications by the Institute for Computer Science and Technology (ICST) of the National Bureau of Standards (NBS).


8. Security of Personal Computer Systems: A Management Guide, Dennis D. Steinauer, NBS Spec. Pub. 500-120, GPO Stock No. 003-003-02627-1.

9. Computer Security Publications, NBS Pubs. List 91, February 1985 (Updated July 1986).

10. FIPS PUB 112 - Standard on Password Usage, March 1985.

11. Guide on Selecting ADP Backup Process Alternatives, Irene Isaac, November 1985 NBS Spec. Pub. 500-134, GPO Stock No. 003-003-02701-4.

12. Technology Assessment: Methods for Measuring the Level of Computer Security, October 1985
W. Neugent, J. Gilligan, L. Hoffman, and Z. Ruthberg
NBS Spec. Pub. 500-133, GPO Stock No. 003-003-02686-7.

13. Security for Dial-Up Lines, May 1986
Eugene Troy
NBS Spec. Pub. 500-137, GPO Stock No. 003-003-02723-5.

14. FIPS PUB 83 - Guideline on User Authentication Techniques for Computer Network Access Control, September 1980.

The following publications and DoN instructions may also be of use:

15. Datapro Reports on Information Security, Datapro Research Corp., Delran, NJ, 1986.

16. Computer Security Handbook, Computer Security Institute, Northborough, MA, 1985.

17. Computer Security Journal, Computer Security Institute, Northborough, MA, Published twice a year.

18. Security Handbook for Small Computer Users, J. Withrow, Air Command and Staff College, Maxwell AFB, Ala. Apr 1985, Report No. ACSC-85-2910, DTIC # AD-A157 091.

19. Data Processing and Communications Security, Assets Protection Publishing Co., Madison Wisc. Published four times a year.

20. Microcomputers: A Security and Recovery Checklist, Assets Protection Publishing Co., Madison Wisc.

21. DoN Automatic Data Processing Security Program, CNO, OPNAVINST 5239.1A, April 1, 1985.

22. Protected Distribution Systems, OPNAVINST 5510.1G

23. Security, Cahners Publishing Company, Magazine Circulation, (303) 388-4511, monthly magazine on general security issues.

24. An Approach to Determining Computer Security Requirements for Navy Systems, Carl E. Landwehr and H. O. Lubbes, Naval Research Laboratory, NRL Report 8897.

25. OMB Circular A-130 [Risk analysis guidelines].

26. The Philip Weights & Associates Security Data Base, $27, a dBASE III database of over 240 computer security products.
170 East 92nd Street, #1B
New York, N.Y. 10128
(212) 410-2434.

## Appendix B. KEY ORGANIZATIONS AND SECURITY CONSULTANTS

Government agencies:

NSA-ISP / NCSC-TSD

| | | |
|---|---|---|
| Maurer, Valerie | (301) 859-4476 | [Navy liaison officer] |
| Chase, William | (301) 859-4463 | |
| Neufeld, Leon | (301) 859-4458 | |
| Duke, Al | (301) 850-7158 | |
| Drake, Earle | (301) 688-7110 | |

NBS-ICST

| | | |
|---|---|---|
| Katzke, Stuart | (301) 921-2705 or 975-2000 | |
| Steinauer, Dennis | (301) 975-3359 | |

GAO-IMTEC

| | |
|---|---|
| Podell, Harold | (202) 275-3210 |

SPAWARS

| | |
|---|---|
| Lubbes, H. O. | (703) 692-8484 |
| Weilminster, Robert | (703) 282-2037 |

NAVDAC

| | |
|---|---|
| Bishop, Chief W. O. | (202) 433-4380 |

DTNSRDC

| | |
|---|---|
| Hays, John | (202) 227-1426 |

Private security consultants (representative sample):

a. Computer Security Institute
   Northborough, MA 01532
   (617) 393-2600

b. Dr. Joel S. Zimmerman
   ComSource 32 Inc.
   Williamsburg, VA
   (804) 253-1512

c. Computer Data Systems
   Huntsville, AL 35805 or Rockville, MD 20850
   (205) 830-1400 (301) 921-7000

d. Total Assets Protection Inc.
   Arlington, TX
   (817) 640-8800

e. Information Systems Security Association, Inc.
   P.O. Box 71927
   Los Angeles, CA 90071

## Appendix C. TRAINING

The following organizations provide training in computer security related topics:

a. Computer Security Institute
Northborough, MA 01532
(617) 393-2600

b. Naval Data Automation Command (NAVDAC)
Contact: Lorena Funderburk, (202) 433-5706
Navy Regional Data Automation Center (NARDAC Washington)
Code 2014
Washington Navy Yard
Washington, DC 20374

c. General Services Administration Training Center
P.O. Box 15608
Arlington, VA 22215-0608
Contact: Roger Melton
(703) 557-1318

d. Physical Security Training Center
Norfolk Naval Shipyard
Portsmouth, VA 23709-5000
(804) 396-3007

e. Interference Control Technologies, Inc. [EMI and TEMPEST]
Don White Consultants, Subsidiary
State Route 625, P.O. Box D
Gainesville, VA 22065
(703) 347-0030

f. R & B Enterprises [EMI and TEMPEST]
20 Clipper Road
W. Conshohocken, PA 19428
(215) 825-1966

g. NCSC-TSD [NSA]
9800 Savage Road
Fort Meade, MD 20755-6000
(301) 859-4500 [Information]
Navy contact: Valerie Maurer [Navy Liaison Officer]
(301) 859-4476
[Courses, training film, and risk analysis expert system]

h. MIS Training Institute
4 Brewster Road
Framingham, MA 01701
(617) 879-7999

i. PDC/Armed Forces Communications & Electronics Association
4400 Fair Lakes Court
Fairfax, VA 22033
(703) 631-6135 / (800) 336-4583

## Appendix D. CONFERENCES

July 13 - 14, 1987
Annual IBM Users Computer Security Workshop
Philadephia, PA
Contact: Computer Security Institute
Northborough, MA 01532
(617) 393-2600

September 13 - 17, 1987
7th Annual Conference on Control, Audit & Security of IBM Systems
Chicago Marriot Hotel
Chicago, IL
Contact: MIS Training Institute
4 Brewster Road
Framingham, MA 01701
(617) 879-7999

September 21 - 24, 1987
Tenth Annual National Computer Security Conference
Baltimore Civic Center
Baltimore, MD
Contact:
Irene Isaac, NBS, (301) 975-3359
Linda Muzik, NCSC, (301) 859-4506
Al Duke, NCSC, (301) 850-7158

September 29 - October 2, 1987
Computer & Communications Security '87 [or INFO Security '87]
Jacob K. Javits Convention Center
New York, New York
Contact: Fred Palumbo
Cahners Exposition Group
999 Summer Street
Stanford, Connecticut 06905
(201) 964-0000

November 9 - 11, 1987
Fourteenth Annual Computer Security Conference
Anaheim Hilton
Anaheim, CA
Contact: Computer Security Institute
Northborough, MA 01532
(617) 393-2600

May 1988 (Date not yet finalized)
Computer and Network Security '88
(Location not yet finalized)
Contact: Linda Leonardt,
Conference Administrator, Institute for International Research
310 Madison Avenue, Suite 1212
New York, NY 10017
(212) 883-1770

## Appendix E. ABBREVIATIONS

| | |
|---|---|
| ASCII | American Standard Code for Information Interchange |
| ADP | Automatic Data Processing |
| ADPPO | ADP Policy Office(r) |
| ADPSO | ADP Security Office(r) |
| ADPSSO | ADP System Security Office(r) |
| CPU | Central Processing Unit |
| DBA | Data Base Administrator |
| DES | Data Encryption Standard private key algorithm |
| DoD | Department of Defense |
| DoN | Department of the Navy |
| DOS<br>MS-DOS<br>PC-DOS | Disk Operating System for 8088/8086/80286/80386 class CPUs by INTEL Corp. PC-DOS is the IBM specific version and MS-DOS is the generic version for the IBM PC look-alikes or clones. The currently active versions are 2.1, 2.11, 3.0, 3.1, 3.2, and 3.3. The next version, OS/2, will be for 80286/80386 CPUs, particularly IBM's new PS/2 series of PCs. It is expected to run in protected mode and allow multitasking and run-time linking. |
| DTNSRDC | David W. Taylor Naval Ship Research and Development Center |
| EMI | Electromagnetic Interference |
| HIU | Host Interface Unit to a local area network |
| Hz | Hertz, cycles per second |
| IBM PC | 16 bit, 8088 based personal computer, usually with two diskette drives, 5 expansion slots, and up to 640 kbytes of directly addressable user memory. It is considered to be the de facto standard for personal business computers. |
| IBM PC/AT | 16 bit (data path), 80286 based personal computer, usually with a 1.2 Mbyte diskette drive and at least 20 Mbytes of fixed disk storage. It allows up to 640 kbytes of user addressable memory in real mode (DOS) and up to 16 Mbytes in protected mode (Xenix). |

| | |
|---|---|
| IBM PC/XT | The latest version is essentially a low end PC/AT. Most likely, this machine will become the bottom of IBM's PC line. The original version, is a PC with 8 expansion slots, a heftier power supply, at least a 10 Mbyte fixed disk, and 256 kbytes on the (PC-2) motherboard. |
| IEEE | Institute of Electrical and Electronics Engineers, Inc. |
| k | Kilo, (prefix for thousand, actual value of 1024). |
| LAN | Local area network |
| MBytes | Megabytes (actual value of one Mbyte is 1,048,576) |
| NBS | National Bureau of Standards |
| NBS-ICST | NBS Institute for Computer Science and Technology |
| NCSC | National Computer Security Center (NSA) |
| NSA | National Security Agency |
| OISSO | Office Information System Security Officer |
| PC | Personal Computer. |
| PIN | Personal identification number |
| PKS | Public key system. This would include any encryption/decryption algorithm where the encryption and decryption keys are different and the encryption key was available to anyone but the decryption key was kept secret. |
| PSO | Physical plant security office(r) |
| RFI | Radio frequency interference (subset of EMI) |
| RPG | Random password generator |
| SA | System administrator |
| SPS | Standby or backup power supply. Off-line backup. |
| TCB | Trusted computing base. The totality of protection mechanisms within a computer system. |
| UL | Underwriters Laboratory |
| UPS | Uninterruptible power supply. On-line backup. |
| WATS | Wide area telephone service |

## Appendix F. DTNSRDC SECURITY PROCEDURES FOR PERSONAL COMPUTERS

The following procedures were adopted by DTNSRDC Code 004 from OPNAVINST 5239.1A:

### OPERATING PROCEDURES FOR CODE_____
### PERSONAL COMPUTER SYSTEM

1. Procedures.

The following operating procedures apply to the _____ personal computer system located in building _____, room _____.

a. Level of Data Processed. No classified information will be processed or stored on the system unless the system is accredited for classified processing and the supplemental operating procedures for processing classified information are followed. Level II data (sensitive unclassified) will be marked and safeguarded in the same manner as "FOR OFFICIAL USE ONLY" data. The system will be used for official business only. The ADP System Security Officer (ADPSSO) will ensure that all users of the system are aware of this restriction.

b. Access Control. Only authorized users will be permitted to operate the personal computer system. Authorized users are verified DTNSRDC employees whose names are contained on an authorized users list created and maintained for the system by the ADPSSO. Additions to the authorized users list will be on an as-required basis and will be subject to approval by the ADPSSO for the system. Periodic reviews of the access list will be made to ensure its accuracy.

c. Media Protection. All software and data files on diskettes will be labeled appropriately and secured during non-working hours. Data files will be protected on a need-to-know basis during periods of operation of the system by other authorized users.

d. Physical Security. If the office space containing the personal computer system is vacant during non-duty hours, doors will be secured and access to the office space will be controlled, or the equipment will be stored in a locked security container, cabinet or desk. As an alternative, the equipment may be secured to desks with commercially available anchor pads, cable locks or similar devices that provide a comparable level of security.

e. Standard Operation Procedures. Start-up, operation, and shutdown of the system shall be in accordance with the procedures provided by the vendor. The system shall be powered off during non-working hours and when not in use or unattended for extended periods of time during working hours.

f. Emergency Procedures. In the event of an emergency, and when time and safety permits, the system will be powered down and files will be secured prior to evacuation.

g. Input/Output Control. All material received for processing and all output products, including magnetic media, will be labeled appropriately and will be protected on a need-to-know basis. Sensitive material will be treated in the same manner as "FOR OFFICIAL USE ONLY".

h. Contingency Plan. A formal agreement should be negotiated with one or more other organizations, with compatible equipment, for contingency use in the event that the system is out of service for an unreasonable period of time. Key files should be backed up periodically if their loss would adversely affect recovery from a contingency situation. Back up files will be stored in a locking file cabinet or locking desk, at a minimum.

i. Training. All users shall have the minimum operational training and shall be briefed by the ADPSSO on security requirements and operating procedures prior to using the system.

j. Documentation. The ADPSSO will ensure that the accreditation support documentation for the system is maintained up-to-date and that a copy of any change is provided to the ADP Security Officer (ADPSO) in Code 004.

k. Enforcement. The ADPSSO is responsible for ensuring that the above procedures are adhered to and that any violations or incidents in regard to the security of the system are reported in writing to the ADPSO. Any significant changes in hardware/software configuration, data classification level, operating mode, etc. may render the ADP security accreditation void and require reassessment of the security posture of the system. Such changes should be closely coordinated by the ADPSSO with the ADPSO.

l. Audit Trails. An audit trail (utilization log) is required for a system authorized to process Level I (classified) or Level II (sensitive unclassified) information and can be maintained either manually or automatically. At a minimum, the audit trail will contain the following information:

(1) Operator's name.

(2) File name(s) accessed (Level I or II files only).

(3) Type of access (create, modify, copy, delete, etc.)

(4) Date/time.

## Appendix G. DTNSRDC ADP SECURITY SURVEY

The following ADP security survey was adopted by DTNSRDC Code 004 from OPNAVINST 5239.1A:

### ADP SECURITY SURVEY
### AND
### ACCREDITATION SUPPORT DATA FORM

The Navy has a substantial investment in ADP equipment, software, data and other ADP resources, and that investment must be protected by an effective ADP security program. The Navy ADP Security Manual, OPNAVINST 5239.1A, is the governing ADP security instruction Navy wide, and replaces or incorporates by reference all other DOD and Navy ADP security instructions. This instruction requires that all ADP systems, networks and office information systems (word processors, etc.) meet minimum security requirements and be accredited.

In the Department of the Navy ADP Security Program, accreditation is the decision of the Designated Approving Authority (DAA) that an ADP facility is operating at a satisfactory level of operational risk. This decision is based on documentation submitted to the DAA from the various steps of the accreditation process - risk assessment, contingency plan, security test & evaluation, TEMPEST vulnerability assessment, security operating procedures, mode of security operation, etc.

This ADP SECURITY SURVEY AND ACCREDITATION SUPPORT DATA FORM is required to be filled out for each ADP system, network and office information system (OIS). The form requires very little writing and is used for the following purposes:

-- to provide basic information to the ADP Security Officer (ADPSO) for listing the ADP system, network or OIS on the DTNSRDC Activity ADP Security Plan Activity Accreditation Schedule as required by OPNAVINST 5239.1A.

-- to provide a checklist and certification that the ADP system, network or OIS meets the minimum security requirements of OPNAVINST 5239.1A, appendix J.

-- to serve as a risk assessment for a less complex facility processing only Level III data.

-- to provide the preparer a checklist for determining the security posture of an ADP facility in preparation for a formal risk assessment.

-- to provide current status of accreditation support documentation.

Sections I, II, and V must be completed for all ADP systems, networks and OIS. Additionally, section III must be completed for all ADP systems and networks which process Level I or II data, and section IV must be completed for all OIS which process Level I or II data. More than one small system, microcomputer or OIS may be listed on the same form provided they process only Level III data, are located within the same office and are protected by the same countermeasures.

Completed forms will be forwarded to the ADPSO, Code 004, via the department ADP System Security Officer (ADPSSO).

ADP SECURITY SURVEY
AND
ACCREDITATION SUPPORT DATA FORM

SECTION I. BASIC DATA. (Applies to all ADP systems, networks and OISs)

1. System Identification: System Name _____

CPU Serial Number _____

( ) Office Information System
( ) ADP System
( ) Network

2. System Description: (List all components, main frames, peripherals, communication processors, encryption devices, remote devices, network and remote interfaces, etc.)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3. Equipment Location: Carderock - Building_____ Room_____

Annapolis - Building_____ Room_____

4. System Operations Contact for Security:

Name: _____ Code: _____

Bldg:_____ Room:_____ Phone:_____

5. Types of Data Processed and Security Modes of Operation

| TYPE OF DATA | PERCENT OF PROCESSING TIME | *SECURITY MODE OF OPERATION |
|---|---|---|
| Level I (Classified) | | |
| SCI | | |
| SIOP-ESI | | |
| TOP SECRET | | |
| SECRET | | |
| CONFIDENTIAL | | |
| Level II (Unclassified Sensitive) | | |
| Privacy Act | | |
| For Official Use Only | | |
| Financial | | |
| Sensitive Management | | |
| Proprietary | | |
| Privileged | | |
| Level III (All Other Unclassified) | | |
| TOTAL | 100% | |

*Security modes of operation as defined in OPNAVINST 5239.1A are: Multilevel, Compartmented, Controlled, System High, Dedicated, Limited Access, N/A.

6. Software - Operating System_____

Programming Language(s)_____

7. Scope of System: (Check all that apply)

( ) Stand-alone and single controlled area (single CPU with single workstation).

( ) Shared logic and single controlled area (single CPU with multiple workstations).

( ) Shared logic and more than one controlled area (single CPU with multiple workstations).

( ) Multiple processors and single controlled area (multiple CPUs).

( ) Multiple processors and more than one controlled area (multiple CPUs).

( ) Used with a remote computer _____ percent of time.

( ) Other:

8. Total Value of System(s): $_____ (Dollar value impact of loss and cost to replace)

A. Equipment: $_____

B. Software: $_____

C. Data: $_____

(Note: dollar values in Table E-2, OPNAVINST 5239.1A can be used as a guideline for computing value of data files.)

9. Mission Relatedness:

A. Primary Function(s) of the System or Network:

_____

_____

_____

B. Contingency Plan Requirement:

( ) Plan is in existence. Date of Plan is _____

( ) Plan is being developed. Estimated completion date is _____.

( ) Plan is not required because loss of processing capability for a reasonable period of time would not adversely affect mission. (Provide statement of justification on separate memorandum)

_____

SECTION II. MINIMUM REQUIREMENTS FOR ENVIRONMENTAL AND PHYSICAL SECURITY.

(Applies to all ADP systems, networks and OISs.)

1. Threat: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

[ ] Adequate heating and controls.
[ ] Adequate cooling and controls.
[ ] Only designated personnel operate controls.
[ ] Functioning temperature and humidity recorder.
[ ] Functioning temperature/humidity warning system.
[ ] Other: _____

Assessment of risk:

[ ] High [ ] Moderate [ ] Low

2. Threat: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

[ ] Adequate primary lighting.
[ ] Adequate emergency lighting.
[ ] Adequate periodic checks of emergency lighting.
[ ] Adequate primary power and outlets.
[ ] Functioning power filters or voltage regulator.
[ ] Available backup power.
[ ] Other: _____

Assessment of Risk:

[ ] High [ ] Moderate [ ] Low

3. Threat: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

[ ] Routine cleaning schedule is adhered to.
[ ] Cleaning personnel are trained in computer room procedures.
[ ] An ADP facility representative is present during cleaning.
[ ] Dust contributors (outer coats, throw rugs, drapes, venetian blinds, etc.) are not permitted in equipment areas.
[ ] Air conditioning filters are cleaned/replaced regularly.

[ ] Floors are polished with non-flake wax using proper buffer materials, or are properly damp-mopped.
[ ] Carpet areas are vacuumed frequently and anti-static spray is used regularly.
[ ] Smoking, eating and drinking are not permitted in equipment areas.
[ ] Other: _____

Assessment of Risk:

[ ] High [ ] Moderate [ ] Low

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

[ ] Water/steam pipes are not located above equipment.
[ ] Water/steam pipes are inspected at regular intervals.
[ ] Functioning humidity warning system.
[ ] Dry-pipe sprinkler system.
[ ] Raised floor.
[ ] Adequate drainage under raised floor.
[ ] Plastic sheets available to cover susceptible equipment.
[ ] Water detection devices.
[ ] Other: _____

Assessment of Risk:

[ ] High [ ] Moderate [ ] Low

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

[ ] Up-to-date fire bill posted.
[ ] Periodic fire drills.
[ ] Training--fire prevention methods.
[ ] Training--emergency power down procedures.
[ ] Training--knowledge of fire detection system.
[ ] Training--use of fire extinguishers.
[ ] Training--use of fire alarm system.
[ ] Training--evacuation plan.
[ ] Training--individual responsibilities in case of fire.
[ ] Functioning emergency power-off switches.
[ ] Sprinkler system installed.
[ ] Halon system installed.
[ ] Carbon dioxide fire extinguishers installed.
[ ] Smoke/heat detectors installed.
[ ] Functioning fire alarm system.
[ ] Emergency exits clearly marked.
[ ] Other: _____

Assessment of Risk:

[ ] High [ ] Moderate [ ] Low

6. Threat: Unauthorized Physical Access.

Operating Countermeasures. (Check all that apply.)

[ ] Perimeter fence.
[ ] Security guards.
[ ] Building secured outside of normal working hours.
[ ] Area alarms (motion detectors, open door detectors, perimeter penetration detectors).
[ ] Authorized personnel access list.
[ ] Recognition of authorized personnel.
[ ] Cypher door lock.
[ ] Combination door lock.
[ ] Closed circuit television.
[ ] Administrative procedures.
[ ] Physical isolation/protection.
[ ] High employee morale.
[ ] Close supervision of employees.
[ ] Indoctrination of personnel in security awareness.
[ ] Other: _____

Assessment of Risk:

[ ] High [ ] Moderate [ ] Low

SECTION III. ACCREDITATION SUPPORT DOCUMENTATION STATUS. (Applies to all ADP systems and networks which will be authorized to handle Level I or Level II data.)

1. All ADP systems and networks which will be authorized to handle Level I or Level II data must either be accredited , or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation including a risk assessment. This section provides a statement of the status of the accreditation support documentation.

2. Accreditation Support Documentation Status. (Check all that apply.)

| In Existence | Being Developed | Required But No Action Taken | Not Required | |
|---|---|---|---|---|
| [ ] | [ ] | [ ] | [ ] | Security Operating Procedures Documentation. |
| [ ] | [ ] | [ ] | [ ] | Line Diagrams Showing Interconnection of Components. |
| [ ] | [ ] | [ ] | [ ] | Description of Installed Countermeasures.** |
| [ ] | [ ] | [ ] | [ ] | TEMPEST Vulnerability Assessment Request. |
| [ ] | [ ] | [ ] | [ ] | Security Test & Evaluation Plan. |
| [ ] | [ ] | [ ] | [ ] | Contingency Plan. |
| [ ] | [ ] | [ ] | [ ] | Risk Assessment. |

** Countermeasures must include those implemented for data protection, and must reflect the mandatory requirements of OPNAVINST 5239.1A including audit trails and password protection where applicable.

SECTION IV. COUNTERMEASURES DOCUMENTATION FOR OFFICE INFORMATION SYSTEMS.
(Applies to all OISs which will be authorized to handle Level I or Level II data.)

Paragraph 4.3 of the DON ADP Security Manual (OPNAVINST 5239.1A) states the security requirements for OISs. For OISs which will be authorized to handle Level I (classified) or Level II (unclassified - sensitive) data, list the operating countermeasures on a separate sheet and make the appropriate certifications below.

1. OISs Handling Level II Data. (Check all applicable blocks.)

[ ] The OIS will be authorized to handle Level II (personal or sensitive business) data. A list of the operating countermeasures is attached. These countermeasures provide proper data protection and audit trails.

[ ] The OIS is a shared logic system with more than one simultaneous user not having need-to-know for all data within the system. Password protection or other equivalent countermeasures are employed for system access and for individual file access.

[ ] The OIS Security Operating Procedures have been documented and submitted to the ADPSO for approval.

2. OISs Handling Level I Data. (Check all applicable blocks.)

[ ] The OIS will be authorized to handle Level I data under a system high or dedicated mode of operation. A list of the operating countermeasures is attached. These countermeasures satisfy the requirements of paragraph 1.2.a and appendix C of the DON ADP Security Manual (OPNAVINST 5239.1A).

[ ] A TEMPEST Vulnerability Assessment has been requested.

[ ] The OIS Security Operating Procedures have been documented and submitted to the ADPSO for approval.

SECTION V. SURVEY DATA

Survey Prepared by:

Name: _____ Code: _____

Building: _____ Room: _____ Phone: _____

To the best of my knowledge, the information provided in this form and the attached documentation is complete and accurate.

Signature: _____ Date: _____

**********

ACCREDITATION REVIEW SYSTEM CPU SERIAL NUMBER _____

1. Department ADP System Security Officer (DADPSSO)

Name: _____ Code: _____

Building: _____ Room _____ Phone: _____

As DADPSSO, I have reviewed these accreditation support data and any attached documentation. Based on these data and other known factors, the following recommendation is made:

[ ] Recommend accreditation.

[ ] Recommend interim authority to operate be granted pending completion of the following actions prior to final accreditation:

---

DADPSSO Signature: _____ Date: _____

2. ADP Security Officer (ADPSO)

Date Received: _____

Action. (Check all applicable blocks.)

[ ] Additional data/documentation requested. Date: _____

[ ] Interim Authority to Operate granted. Date: _____

[ ] Level I accreditation granted. Date: _____

[ ] Level II accreditation granted. Date: _____

[ ] Level III accreditation granted. Date: _____

## Appendix H. DTNSRDC CONTINGENCY PLAN FOR PERSONAL COMPUTERS

The following contingency plan was adopted by DTNSRDC Code 004 from OPNAVINST 5239.1A:

From: _____, Code _____
To: Designated Approving Authority (DAA)
Via: ADP Security Officer (004)

SUBJ: CONTINGENCY PLAN FOR ADP SYSTEM

Ref: (a) OPNAVINST 5239.1A

1. Reference (a) requires that a contingency plan be developed for the_____System located in _____.

This ADP System is used primarily for _____

_____.

**********
** CHECK EITHER PARAGRAPH 2 OR 3. **
**********

[ ] 2. In the event this ADP system becomes inoperative, a compatible system _____ located in _____ will be used on a time sharing basis to accomplished the required tasks.

Point of contact for the backup system is _____.

[ ] 3. In the event this ADP system becomes inoperative, this unplanned disruption of service will not have a critical impact on the mission. Therefore, no contingency plan is required.

DATE_____ _____
(Signature)

## REFERENCES


1. Zimmerman, Dr. Joel S., "PC Security: So What's New?," DATAMATION, Vol. 31, No. 21, pp. 86-92 (1 Nov 1985).

2. "DoD Trusted Computer System Evaluation Criteria," DOD 5200.28-STD (Dec 1985).

3. "Information Security Products and Services Catalogue," NSA, (April 1987, published quarterly).

4. "Personal Computer Security Considerations," NCSC-WA-002-85, (Dec 1985).

5. Hoffman, Lance J., "PC Software for Risk Analysis Prove Effective," Government Computer News, pp. 58-59 (27 Sep 1985).

6. Datapro Reports on Information Security, Datapro Research Corp., (1986).

7. Landwehr, Carl, E. and H. O. Lubbes, "An Approach to Determining Computer Security for Navy Systems," NRL Report 8897 (13 May 1985).

8. Levine, Arnold S., "Consider Different Approach for Measuring Security," Government Computer News, p. 64 (29 Aug 1986).

9. Steinauer, Dennis D., "Protecting Our Resources," Government Data Systems, pp. 19-25 (Nov/Dec 1984).

10. Schlosberg, Jeremy, "Out of Site," Digital Review, pp. 37-41 (March 1985).

11. Goldstein, Andy, "Operating Systems Offer Security Features To Control Computer Access," Computer Technology Review, pp. 191-199 (Winter 1985).

12. Rivest, R. L., A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Crypto System," Communications of the ACM, pp. 120-126, (Feb 1978).

13. Call, Barbara, "Security Needs," PC Week, pp. 77-83 (29 July 86)

14. "Public Key Technology vs. DES - Which is for You?", Bulletin on Information Security, Number 101, Analytics Communications Systems, (ACS), Reston, Va. (1983).

15. Baker, Gary, "For LANS Only - Diskless Machines Are Made To Run On Networks," LAN Magazine, pp. 49-54, (Jan 1987).

16. Rosch, Winn L., "Backup Power, When the Juice Stops Flowing," PC Magazine, pp. 181-212, (16 Sept 1986).

## INITIAL DISTRIBUTION

| Copies | | | |
|---|---|---|---|
| 1 | USASAC | AMC-SA3 | D. Murtomaki |
| 1 | NAVSUP | 0412 | R. Bell |
| 1 | NAVSUP | PML5505 | H. Lieberman |
| 1 | NAVSUP | 0433 | G. Ramick |
| 2 | DTIC | | |

## CENTER DISTRIBUTION

| Copies | Code | Name |
|---|---|---|
| 1 | 004 | J. Hayes |
| 1 | 05 | Capt. B. Sack |
| 1 | 055 | G. Brown |
| 1 | 18 | Dr. C. Schoman |
| 1 | 182 | A. Camara |
| 1 | 1824 | Dr. S. Berkowitz |
| 20 | 1824 | I. Zaritsky |
| 1 | 184 | J. Schot |
| 1 | 185 | R. Schaffran |
| 1 | 187 | M. Zubkoff |
| 1 | 189 | G. Gray |
| 2 | 189 | P. Hayden |
| 1 | 522.1 | TIC (C) |
| 1 | 93 | L. Marsh |

## DTNSRDC ISSUES THREE TYPES OF REPORTS

1. **DTNSRDC reports, a formal series,** contain information of permanent technical value. They carry a consecutive numerical identification regardless of their classification or the originating department.

2. **Departmental reports, a semiformal series,** contain information of a preliminary, temporary, or proprietary nature or of limited interest or significance. They carry a departmental alphanumerical identification.

3. **Technical memoranda, an informal series,** contain technical documentation of limited use and interest. They are primarily working papers intended for internal use. They carry an identifying number which indicates their type and the numerical code of the originating department. Any distribution outside DTNSRDC must be approved by the head of the originating department on a case-by-case basis.

END

11-87

DTIC